Common Criteria

Evaluation and Validation Scheme

For

Information Technology Security

Guidance to Validators of IT Security Evaluations

Scheme Publication #3

Version 1.0

February 2002

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Systems Security Organization
9800 Savage Road
Fort George G. Meade, MD 20755

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
01-02-2002		xx-xx-2002 to xx-xx-2002

4. TITLE AND SUBTITLE
Common Criteria Evaluation and Validation Scheme for Information Technology Security: Guidance to Validators of IT Security Evaluations Version 1.0
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
National Institute of Standards and Technology, National Security Agency
100 Bureau Drive
Gaithersburg, MD20899

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The purpose of this document, Guidance to Validators of IT Security Evaluations, is to provide guidance and assistance to Validators in performing their assigned duties under the Validation Body. Additionally, the document provides information to the CCTLs and sponsors of evaluations about the activities and responsibilities of assigned Validators.

15. SUBJECT TERMS
IATAC COLLECTION; information security; common criteria; vulnerability assessment

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Public Release	112	Fenster, Lynn lfenster@dtic.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	2/1/2002	Report 2/1/2002

4. TITLE AND SUBTITLE
Common Criteria Evaluation and Validation Scheme for Information Technology Security: Guidance to Validators of IT Security Evaluations Version 1.0

5. FUNDING NUMBERS

6. AUTHOR(S)
Unknown

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Institute of Standards and Technology, National Security Agency
100 Bureau Drive, Gaithersburg, MD 20899

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

The purpose of this document, Guidance to Validators of IT Security Evaluations, is to provide guidance and assistance to Validators in performing their assigned duties under the Validation Body. Additionally, the document provides information to the CCTLs and sponsors of evaluations about the activities and responsibilities of assigned Validators.

14. SUBJECT TERMS
IATAC Collection, information security, common criteria, vulnerability assessment

15. NUMBER OF PAGES
111

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

(This page intentionally left blank)

Table of Contents

(This page intentionally left blank)

1 Introduction

The National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) for Information Technology Security was established by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to validate conformance of Information Technology (IT) products and protection profiles (PP) to international standards. Currently, the CCEVS scope covers information technology products and protection profiles evaluated for compliance to the *Common Criteria for Information Technology Security Evaluation* (CC) for any assurance package made up of components found in Evaluation Assurance Levels (EALs).

The principal participants in the CCEVS program are the following:

- **Sponsor**: The Sponsor may be a product developer or a protection profile developer, a value-added reseller of an IT security-enabled product or protection profile (PP), or another party that needs to have a product or PP evaluated. The sponsor requests that a Common Criteria Testing Laboratory conduct security evaluation of an IT product or protection profile.
- **Common Criteria Testing Laboratory (CCTL)**: The CCTL is a commercial testing laboratory accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS to perform security evaluations against the *Common Criteria for Information Technology Security Evaluation* (CC) using the *Common Methodology for Information Technology Security Evaluation* (CEM).
- **CCEVS Validation Body**: The CCEVS Validation Body hereafter referred to as the Validation Body, is the organization established within NIAP to implement and operate the evaluation and validation scheme for the U.S. Government.

1.1 Purpose

The purpose of this document, *Guidance to Validators of IT Security Evaluations,* is to provide guidance and assistance to Validators in performing their assigned duties under the Validation Body. Additionally, the document provides information to the CCTLs and sponsors of evaluations about the activities and responsibilities of assigned Validators.

The Validation Body operates under a quality system to ensure that the evaluation and validation activities taking place within the Validation Body are being conducted in accordance with the provisions of the *Common Criteria for Information Technology Security Evaluation (CC),* the *Common Methodology for Information Technology Security Evaluation (CEM),* the *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security* (CCRA), and any CCEVS-specific policies and procedures. The Validation Body reviews all CCTL evaluation reports, and other materials as needed, to ensure that the selected evaluation criteria and evaluation methods have been correctly applied. The Validation Body monitors evaluations in progress to issue additional guidance or clarify evaluation results.

Validation is the independent confirmation that an IT security evaluation has been conducted in accordance with the provisions of the CCEVS, and that the conclusions of the CCTL are consistent with the facts presented and are documented in the CCTL Evaluation Technical Report

(ETR). Validation involves confirming the CCTL evaluation results, preparing the validation report, and issuing a Common Criteria Certificate. To accomplish validation, the Validation Body assigns a person known as a Validator for each IT security product or PP under evaluation.

1.2 Scope

This *Guidance to Validators of IT Security Evaluations* document is one of a series of technical and administrative CCEVS publications that describe how the Validation Body operates. This document complements or references other CCEVS publications and documents used in the operation of the CCEVS. The Guidance *to Validators of IT Security Evaluations* also references other documents such as Common Criteria, NVLAP and ISO publications in describing guidance to Validators. The reader of the *Guidance to Validators of IT Security Evaluations* will need to be familiar with these reference documents for an understanding of the Validator guidance described herein. Copies of the CCEVS, NVLAP, Common Criteria publications, and other CCEVS related information is available through the CCEVS web site http://niap.nist.gov/cc-scheme.

This document describes the approach used by the Validation Body to validate the CCTL evaluation results of an IT security product or a PP evaluation. The scope of Validator guidance provided in this document is expressed both in terms of the evaluation/validation process, and in terms of the types of validation activities required for validation of an IT product or PP.

Validator guidance for the entire validation process from CCTL Evaluation Acceptance Package (EAP) submission through validation wrap up is described. There are guidelines when validation activities occur, and recommendations for interactions between the Validator and other parties involved in the process. Assignment of a Validator to an evaluation, and the process for providing the Director of the CCEVS Validation Body with a recommendation for issuing a Common Criteria Certificate after completion of the validation report are also described.

The validation activities required for validation of CCTL evaluation results varies depending on laboratory experience, IT product technology, number of CC components or work units, reuse of evaluation material from previous validations, and detail of information provided in CCTL work plans, procedures, records and Evaluation Technical Report (ETR). This document also describes the Validators responsibilities for validation record keeping, and for post-validation feedback to the Validation Body for improving CCEVS and CCTL procedures.

1.3 Organization

This document is organized to provide the reader with an understanding of the validation process and activities that are used within the Validation Body.

Chapter 1 provides introductory information that defines the purpose and scope of the validation process.

Chapter 2 provides an overview of the validation process and the Validator responsibilities for validating the CCTL evaluation results.

Chapter 3 describes the purpose and applicability of the CCTL's Quality System to validation activities.

Chapter 4 describes the preparation phase of the validation process.

Chapter 5 describes the validation activities occurring during the validation conduct phase to confirm correct and consistent application of the CC and CEM in CCTL evaluations.

Chapter 6 describes the conclusion phase of the validation process.

Chapter 7 provides an overview of validation records that the Validators must keep for the CCEVS quality system.

Chapter 8 describes the validation support mechanisms that are available to aid Validators in execution of their duties.

Four Annexes provide acronyms, definitions, validation guidance for CEM work units, and validation record formats.

(This page intentionally left blank)

2 Validation Process and Validator Responsibilities

2.1 Validation Goals

The Validation Body has established validation processes to ensure that CCTL evaluations are performed with the quality and independence that is expected by the users of IT products and protection profiles.

The validation processes support quality by ensuring that CCTLs are consistently and properly applying the appropriate methods and techniques during an evaluation. The validation processes support independence by ensuring that evaluations are conducted impartially. The validation processes used by the CCEVS are intended to use resources available to the Validation Body in a manner that will ensure evaluation quality and independence.

With respect to quality, a primary goal of validation is to ensure correct and consistent evaluations of Target of Evaluations (TOEs) and Protection Profiles (PPs). Correctness refers to the application of evaluation criteria and evaluation methodology by the CCTLs in accordance with the CC, CEM and associated Common Criteria Interpretation Management Board (CCIMB), and CCEVS formal interpretations. Consistency refers to the attainment of similar evaluation results when similar TOEs or PPs are evaluated by the same CCTL or by different CCTLs. Because each CCTL operates under its own quality system for performing evaluations, and because there may be different skill levels even among teams from the same CCTL, the Validators must apply appropriate measures to ensure correct and consistent evaluation results.

2.2 Validation Activities

Validation activities are used for determining that the results of the evaluation analysis are technically correct and consistent with the CC and the CEM. Validation activities fall within the broad categories of 1) Review, 2) Monitor, 3) Witness/Observe, and 4) Report/Document.

Validators are responsible for reviewing the CCTL evaluation results, not for performing the evaluation. Validation activities shall focus on reviewing the Evaluation Work Plan, ST or PP, CCTL work records and the ETR in assessing the CCTL's application of the CC and the CEM. In determining complete, correct and consistent evaluation of a TOE or PP, the Validator may apply additional validation activities in validating the CCTL evaluation results. These additional activities can include:

(a) Reviewing CCTL evaluation procedures,
(b) Interacting and holding discussions with evaluation teams,
(c) Monitoring CCTL evaluation meetings,
(d) Observing CCTL testing activities
(e) Reviewing evaluation evidence in response to CCTL-generated questions, comments, or records.

Validators are expected to conduct only those validation activities that are necessary to confirm correct and consistent application of the CC and CEM, and to determine that a thorough analysis of the TOE or PP was performed. The set of activities applied depends on the assurances selected for the evaluation, the technology being evaluated, and the level of detail in the CCTL's procedures and records.

2.3 Validation Process Overview

The validation process is used to assess whether evaluation of a TOE or PP has conformed to the standards required by the CCEVS. The evaluation process is intended to produce a correct and technically sound result every time. However, there is subjectivity involved in the evaluation process because evaluators make subjective judgements about the adequacy of each piece of evaluation evidence. The validation process and associated activities are designed to confirm that the CCTL has performed the evaluation within the acceptable bounds of subjectivity and that the evaluation results are consistent with what would be obtained by a different CCTL evaluating the same product.

The Validation body will assign a Validator for each CCTL evaluation. The Validation Body may also assign a Validator backup/assistant or Validator trainee to work with the Validator. The Validator will serve as the liaison between the Validation Body and the CCTL. At all levels of assurance, the Validator must be proactive to ensure adequate interaction with and support to the evaluation team. The Validator's role is to determine that the evaluation was thorough, technically sound, and conducted in accordance with CCEVS requirements. Further, the Validator's role is to promote quality in CCTL evaluations, and the validation activities should not impede the CCTL's ability to conduct the evaluation.

The validation process is accomplished in three phases: Preparation, Conduct, and Conclusion. A summary of each phase is described below.

2.3.1 Preparation

The starting point for all validations is the Evaluation Acceptance Package submitted by a CCTL. This package must contain an Evaluation Work Plan, a Security Target or Protection Profile, and identify the points of contact for the CCTL and the sponsor of the evaluation. The Validator must review the Evaluation Acceptance Package and use this information to develop a corresponding Validation Plan that outlines the expected validation activities for the evaluation. Before completing the Validation Plan, the Validator may need to schedule an orientation meeting with the CCTL to gain an understanding of the CCTL's evaluation procedures, records and record keeping system. This orientation should address the form and content of only the evaluation procedures and records that will be used by the CCTL for the evaluation. The CCTL evaluation procedures and record keeping information should be considered in selecting validation activities and in the formulation of the Validation Plan.

For evaluation acceptance, the Validator will coordinate and hold an Evaluation Acceptance Kick-Off meeting with the CCTL and the Sponsor. The purpose of the Evaluation Acceptance Kick-Off meeting is to introduce the CCTL, Validation Body and Sponsor representatives to each other,

and to promote an understanding among the participants of each organization's roles, expectations and plans for the evaluation. Once this meeting has occurred and all parties are in agreement, the Validation Body, CCTL, and Sponsor sign an *Evaluation Acceptance and Non-Disclosure Agreement* affirming that the evaluation has been officially accepted for validation processing by the Validation Body and that evaluation activities may proceed.[1]

2.3.2 Conduct

After an evaluation has been officially accepted for validation processing by the Validation Body, the conduct phase begins. The CCTL should conduct all evaluation activities in accordance with CEM, Evaluation Work Plan, and CCEVS process. The Validator shall simultaneously monitor CCTL activities, provide guidance as needed, and conduct validation activities in accordance with the Validation Plan and this guidance document.

In conducting validation activities, the Validator must rely upon available resources such as the Evaluation Work Plan, the CCTL's record keeping system, physical observations, the ETR, and when necessary, evaluation evidence. The Validator should not perform the evaluation, but should verify that the CCTL conducted the evaluation in accordance with the CEM, that the CCTL applied the Common Criteria properly, and gain confidence that the CCTL analysis of the evaluation evidence supplied supports the conclusions reached.

A requirement for evaluation procedures and record keeping is part of every CCTL quality system. The Validator needs to have an understanding of the evaluation procedures and records that the CCTL will use for the specific evaluation that the Validator will be overseeing. The Validator reviews the evaluation procedures and records as needed to confirm the CCTL's adherence to the CC, CEM and CCEVS requirements.

Upon completion of the evaluation, the CCTL provides the Validator with a complete Security Target or Protection Profile, an ETR, all evaluation Observation Reports (ORs) along with corresponding Observation Decisions (ODs), and a draft Validated Products List (VPL) Entry. The Validator will review these materials, and interact with the team to resolve any issues identified by the Validator.

2.3.3 Conclusion

In the conclusion phase, the Validator uses the final CCTL evaluation materials from the conduct phase to produce a Validation Report and a recommendation for issuing a certificate. The draft Validation Report, draft Common Criteria Certificate information, and VPL Entry information will concurrently be submitted to the CCTL and to the Sponsor for review of accuracy and for approval to release the validation information. The Validation Body will review the validation material and the recommendation of the Validator and, if appropriate, will issue a Common

[1] If a CCTL begins an evaluation before obtaining official acceptance for validation processing by the Validation Body, the Validation Body may require some evaluation process steps be re-started from the beginning in order for the Validator(s) to perform their functions.

Criteria Certificate and post the VPL entry to the VPL. As part of the Post–Mortem validation activities, other Validation Body members may review the validation report. The purpose of the review is to enable discussions with the Validator about the technical validation decisions that were made, and whether these decisions should be promulgated throughout the Validation Body.

2.4 Validator Responsibilities

Validators must understand their responsibilities within the CCEVS. The primary responsibility assigned to a Validator is to monitor an evaluation and validate evaluation results. Other responsibilities of the Validator include serving as CCEVS representative, validation project coordinator, and CCTL support.

2.4.1 Validate Evaluation Results

The Validator will perform the following quality management activities in validating evaluation results:

- Verify that planned evaluation activities, methodologies and procedures are feasible and appropriate;
- Verify that the Common Criteria and the Common Evaluation Methodology are consistently and correctly applied in evaluations;
- Review documented evaluation results, verdicts and rationales for technical accuracy and completeness;
- Review the ST or PP, as appropriate, for correct application of the CC;
- Attend internal CCTL reviews of milestone activities to discuss findings;
- Provide answers and direction to the CCTL for the conduct of the evaluation when these responsibilities are within the Validator's scope of authority;
- Consult with Chief Validator, when necessary, to gain informal input/guidance relative to technical and/or process issues;
- Comment on Observation Reports (ORs) and assist the Chief Validator in understanding the issues associated with the OR;
- Review ORs submitted to the CCEVS to ensure that observations, problem descriptions, proposed resolutions, decisions, or interpretations are correctly and sufficiently described;
- Review draft ETR sections as they are completed and review the final version of the ETR for accuracy and completeness; and
- Review evaluation records as needed to confirm accuracy or completeness of evaluation reporting.

2.4.2 CCEVS Representative

The Validator serves as the primary CCEVS representative interfacing with the CCTL for the conduct of an evaluation. As CCEVS representative the Validator should:

- Serve as CCEVS central point of contact between the CCEVS and the CCTL;
- Confirm the evaluation team is aware of the latest applicable CCEVS policies, procedures, and guidance documents;
- Confirm the evaluation team is aware of the latest applicable Common Criteria and CEM interpretations and precedents;
- Maintain awareness of and apply the latest CCEVS policies and procedures;
- Inform Validation Body management of any deviations from, or needed changes to CCEVS policies and procedures;
- Inform Validation Body management of issues adversely affecting credibility of evaluations and CCEVS operations;
- Report evaluation-related quality issues to Validation Body management;
- Forward Observation Reports (ORs) to the Chief Validator;
- Forward Observation Decisions (ODs) to the evaluation team;
- Forward evaluation team's questions to CCEVS regarding CCEVS policy, procedures, schedules, and decisions; and
- Coordinate with the Records Manager to notify the evaluation team and CCTL management when the Validation Body has approved the final VPL entry, thereby indicating that validation of the CCTL evaluation activities is completed.

2.4.3 Validation Project Coordinator

As the validation project coordinator, the Validator should:

- Manage and/or coordinate assigned validation project activities;
- Forward to Validation Body the final ETR, Security Target, draft Validated Products List entry, and all Observation Reports (ORs) and their corresponding Observation Decisions (ODs) after the evaluation has been completed and reviewed;
- Prepare and submit validation records to CCEVS to document validation activities in accordance with CCEVS requirements and formats; and
- Present the results of the validation activity in Validator review meetings when requested to do so.

2.4.4 CCTL Support

The Validator should support the CCTL to both facilitate the evaluation and to enhance the capabilities of the CCTL. This support may be in the form of technical advice to the CCTL in areas such as information technology and evaluation methodologies. In performing this role the Validator must always maintain a fair and open environment for competition between CCTLs. To provide such advice, the Validator must have sufficient technical understanding of the objectives of the evaluation and hence may need to have access to evidence produced by the sponsor and the evaluator. The Validator is responsible for protecting such information appropriately.[2]

[2] Access to this information may be accomplished by possessing the actual documentation, although it could be granted in other ways (e.g., at the evaluation facility, on-line, etc.).

As CCTL technical support, the Validator should:

- Meet, teleconference, or otherwise communicate with the evaluation team as needed;
- Participate in product training if it is provided and available;
- Confirm the evaluation team is aware of applicable evaluation techniques, practices, test methods, processes and procedures available to all CCTLs;
- Suggest, where appropriate, the type of information that should be included in ETRs and records to enable efficient and effective validation of evaluation results;
- Make note of good nonproprietary evaluation techniques, practices, test methods, processes and procedures obtained either from evaluation/validation experiences or general education and investigation for CCEVS to develop written guidance for distribution to all CCTLs; this is particularly important for new security technologies.

3 NVLAP & CCTL Quality System Role in Validations

3.1 NVLAP and ISO Standards Overview

The CCEVS policies, procedures and concept of operations are built upon and guided by documents issued by the International Organization for Standardization (ISO) and the National Voluntary Laboratory Accreditation Program (NVLAP). These include ISO Guide 65, NIST Handbooks 150 and 150-20, and the ISO 9000 series standards. The purpose of this section is to provide a brief overview of the NVLAP and ISO 9000 concepts to promote understanding of how the CCTL quality system is expected to be used by Validators in performing their validation activities. This section also describes the Validator's role, and differentiates that role from the other roles of CCTL evaluator and NVLAP laboratory assessor. This section addresses only the parts of ISO 9000 that are of primary interest to Validators.

NVLAP is designed to be compatible with domestic and foreign laboratory accreditation programs in order to ensure the universal acceptance of test data produced by NVLAP-accredited laboratories. In this regard, the NVLAP procedures are compatible with, among others, the most recent official publications of ISO/IEC 17025 (formally ISO/IEC Guide 25), ISO Guides 2, 30, 43, 45, 49, 58, and ISO standards 8402, 9001, 9002, 9003, and 9004 documents. The criteria in NIST Handbook 150 encompass the requirements of ISO/IEC Guide 17025 and the relevant requirements of ISO 9002-1994. NVLAP Handbook 150-20 contains information that is specific to Common Criteria testing and interprets the Procedures and General Requirements of NVLAP Handbook 150 where appropriate.

To become NVLAP accredited CCTLs must develop, use and maintain a quality system. The CCTL Quality System encompasses the policies, organization, responsibilities, procedures, processes, and resources that the CCTL use to produce a product that is of consistent quality and that meets defined requirements. The CCTL Quality System describes how the CCTL intends to operate, and provides the documentation of operating activities to enable verification of adherence to the quality system, and to the CC, CEM and CCEVS requirements. Through the use of audits and management reviews, the CCTL improves its quality system and its service to its customers.

3.2 Quality System Documentation Pyramid

NVLAP and associated ISO 9000 documents require that the CCTL Quality Systems be documented. The types of documentation found in quality systems include a Quality Manual, and various categories/levels of procedures, instructions, records, forms, reports, etc. Figure 3-1 below shows the documentation pyramid used for describing ISO-9000 based quality systems.

Figure 3-1: Quality System Documentation Pyramid

- **Quality Manual**: The Quality Manual is the top-level document that states policy, describes the overall quality system, states management commitment, defines authorities and responsibilities, outlines implementation and points to procedures.

- **System-Level Procedures**: System-Level Procedures are high-level instructions that describe how things move through the organization and how the system is implemented, including operating controls for quality processes and systems and interdepartmental (cross-functional) flows and controls (i.e., who, what, where and why). System-Level Procedures may reference other documentation such as specific instructions.

- **Instructions**: Instructions, both technical and work instructions, are intradepartmental, and describe how daily jobs are done. They contain information on topics that include how to perform specific duties, prepare forms, and handle intradepartmental activities.

- **Records**: Records are the documentation of evidence of activities performed or results achieved, which serve as a basis for verifying that the organization is doing what they say they intend to do. Records include forms, reports, etc.

Each level of the documentation pyramid provides the basis for building documents for the next level; that is, the Quality Manual forms the bases for describing system-level procedures, the system-level procedures define the basis for detail operating instructions, the instructions identify the records that are to be kept.

A quality system contains many different categories of procedures, instructions and records. The various procedures, instructions and records may address distinct areas of the quality system such as contracting, training, auditing, testing, etc.

3.3 CCTL Quality System

3.3.1 Overview

A "quality system" is defined as the organizational structure, responsibilities, procedures, processes, and resources for implementing quality management. Each CCTL must establish, use, and maintain a quality system appropriate to the type, range, and volume of activities that it undertakes. Each CCTL must conduct audits of its activities, at appropriate intervals, to verify that its quality system contains adequate and up-to-date documents, including the Quality Manual, Procedures, Instructions, Records, Reports, and Forms. Regardless of its shape or form, all elements of the quality system must be documented and available to CCEVS personnel.

The CCEVS will use various elements of the CCTL Quality System for fulfilling its validation responsibilities under the CC, CEM and CCRA. The following paragraphs provide guidance to Validators on how to use information from the CCTL Quality System. A conceptual view of a documented CCTL Quality System is provided in Figure 3-2.

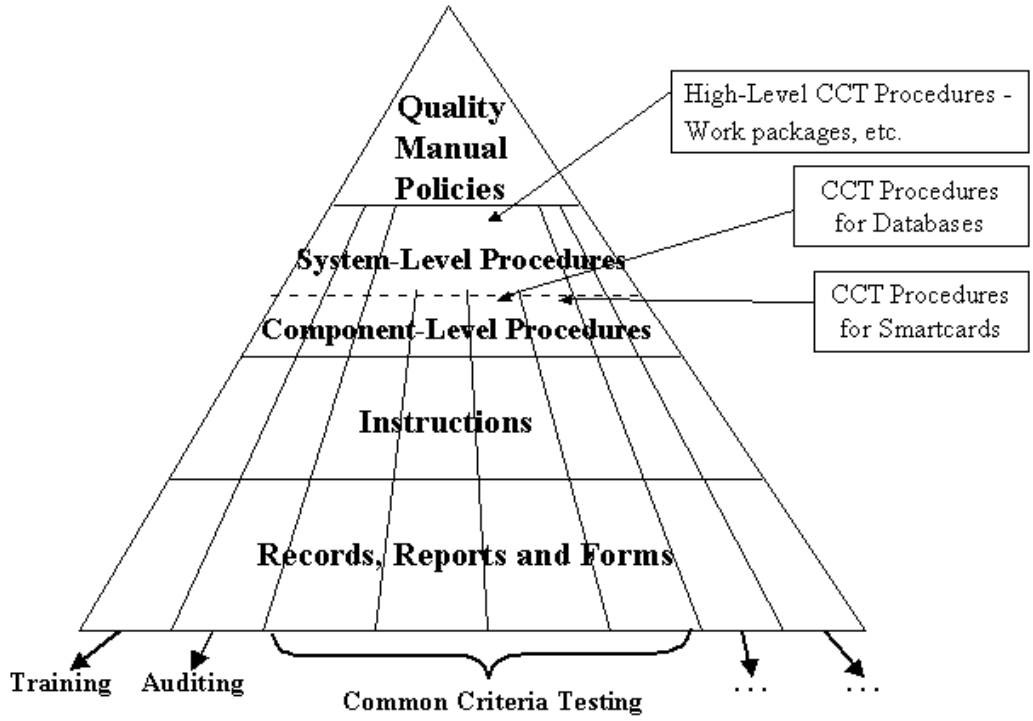

Figure 3-2: Conceptual View of CCTL Documented Quality System

3.3.2 Focus Areas for Assessors, Evaluators and Validators

The CCTL Quality System is intended to support three primary parties identified by the CCEVS. The quality system provides the CCTL evaluators with the organization, responsibilities, procedures, processes, and resources that the CCTL uses to produce a product of consistent quality that meets defined requirements; provides the NVLAP assessors with information for assessing compliance to laboratory accreditation requirements; and provides the CCEVS Validator with information for determining adherence to CC, CEM and CCEVS requirements. The roles of the assessor, evaluator, or Validator focusing on the CCTL Quality System differ for each in the performance of the duties of that role.

- **Assessor Focus**: Quality Manual, and Different Types of Procedures, Instructions and Records

  The NVLAP Assessor typically focuses on assessing laboratory competence, and on the overall scope of implementation, use and auditing of all levels of the quality system documentation pyramid. The Assessor does not look at every procedure, instruction or record, but instead looks for the presence of all quality systems critical elements and evidence of use. The Assessor reviews items such as quality manuals, audits, complaints, procedures, etc.

- **Evaluator Focus**: Detail Application of All Elements of the CCTL Quality System

  The Evaluator typically focuses on the customer's product and the details for all elements of all levels of the Quality System documentation pyramid.

- **Validator Focus**: Common Criteria Testing Procedures, Instructions and Records

  The Validator typically focuses on the three lower levels of the quality system documentation pyramid, which are concerned with procedures, instructions and records (i.e., the documentation produced by the CCTL) for Common Criteria Testing. A CCEVS objective is that the Validator can use the "products" of the CCTL Quality System (i.e., reports, procedures, instructions and records) as the primary evidence for confidence building, and for determining conformance to CC, CEM and CCEVS requirements. The Validator only needs to look at the CCTL common criteria testing procedures, instructions and records that are applicable for the evaluation in question. The Validator can look at other parts of the CCTL's Quality System to aid in general understanding of the CCTL's Quality System approach, but should not assess the CCTL's Quality System. An assessment of the CCTL's Quality System is performed by NVLAP as part of the laboratory accreditation activities.

3.4 CCTL Evaluation Procedures and Instructions

Each CCTL is expected to conduct evaluations in accordance with the Common Criteria Testing procedures established in their Quality System. The Validators should review the CCTL procedures and instructions to verify that the evaluation approach is consistent with requirements of the CC, CEM, and CCEVS, and that the procedures and instructions are appropriate for the

technology and product being evaluated. The procedure review enables the Validator to gain technical confidence in the laboratory's evaluation processes.

The CCTL Quality System procedures are expected to continually evolve over time. The Validators should remain aware of this anticipated evolution and should continually seek the latest procedures from the CCTL when conducting validation activities.

NVLAP accreditation of a CCTL is based on (1) the laboratory's demonstrated competence in performing CC evaluations, and (2) the laboratory's demonstrated capability to mature its Quality System through continued improvement and population of procedures, instructions and records. The number and quality of CCTL Quality System procedures and instructions are expected to increase/improve as the CCTL gains experience from conducting evaluations, and as it finds more effective ways to do testing.

In addition, the CCTL Quality System procedures and instructions are expected to evolve due to changes in the type, range, and volume of activities or evaluations the CCTL undertakes. As security technologies evolve, new and modified procedures will be needed. The Validator should allow for this type of evolution, and should expect to work with concepts, notes, or drafts of documented procedures and instructions as they are being documented by the CCTL.

3.5 CCTL Evaluation Records

Each CCTL is expected to keep records of evaluation activities as defined within their quality system. The validation procedures used by the CCEVS are highly dependent upon the CCTL's Quality System being effectively implemented with comprehensive records.

A CCTL is expected to submit a work plan to the CCEVS as part of the evaluation acceptance package. A specification list of CEM work packages that are to be performed during the evaluation should be included in the work plan. As these work packages are completed, the results should be entered as records into the CCTL's Quality System.

The records for each work package should contain both the plan and results of work performed. The plan should include the objective, required inputs, expected outputs, and techniques that will be used for the activity. These may be drawn from other sources within the quality system, such as written CCTL procedures or the CEM.

The recorded results are the complete written analysis or other actions performed by the CCTL to complete the work package. The record should also contain information about the findings, the persons who performed the work and the dates during which that work was performed.

The above paragraphs specifies the type of information that the Validation Body expects to be contained within those records so that Validators can perform their role as required by the CCEVS.

In order for the Validators to accomplish their tasks, they must have access to all the records related to technical activities of the evaluation. The CCTL is expected to provide these records to the Validator in an appropriate and timely manner.

(This page intentionally left blank)

4 Preparation Phase

In the preparation phase the Validator must plan the activities to be used in validating the results of a CCTL evaluation of a TOE or PP. In order to prepare a plan, the Validator must review the ST or PP, the Evaluation Work Plan, Annex C-Validation Guidance for CEM Work Units, CCTL procedures, and CCEVS and CCIMB interpretations. The Validator must schedule an Evaluation Acceptance Kick-off meeting, produce a Validation Plan, and document all reviews and meetings. The preparation phase concludes with the Chief Validator reviewing and approving the Validation Plan, the CCTL and the Sponsor signing an evaluation acceptance and non-disclosure agreement, and the Sponsor signing a statement of approval or disapproval to publicly list the product or PP as "In Evaluation". The sections below identify the validation activities, and how they are applied to the validation preparation phase.

4.1 Reviews

4.1.1 Security Target

For the preparation phase the Validator must review the provided ST to determine if it is "substantially complete." A substantially complete ST will have information in all of the sections of the ST [TOE Introduction, TOE Description, TOE Environment (to include Assumptions, Threats, and Organizational Security Policies), Security Objectives, TOE requirements (to include functional and assurance requirements), the TOE Summary Specification, any PP Claims, and the Rationale where appropriate.[3]]. While it is understood that more information may be added, or information may be modified as the TOE is evaluated, there should be enough content in the ST to allow the Validator to make a preliminary assessment of the viability of the ST to serve as a specification for a TOE evaluation.

4.1.2 Protection Profile

For a PP evaluation the Validator shall review the candidate PP to determine if it is "substantially complete." Because the evaluation activity will focus on a detailed review of the PP, the Validator's review of the PP in the preparation phase is simply a review to determine that sufficient information is contained in all sections of the PP.

[3] For instance, if the ST contains no "organizational security policies" it is allowable for the ST not to have any information in that portion of the TOE environment section.

4.1.3 Evaluation Work Plan

The Validator must review the Evaluation Work Plan. The goal of this review is to determine, given the state of either the ST or PP, whether the milestones appear to be appropriate for the assurance level chosen and the complexity of the TOE or PP. For a TOE evaluation this is only a rough estimate because a large factor will be the state of the ADV, ATE, and AVA documentation supplied by the vendor, which will not be known (by the Validator) until the evaluation activity has begun.

During the preparation phase, the Validator must confirm that the work packages listed in the Evaluation Work Plan are consistent with the assurance requirements identified in the ST. The Validator should also review the Evaluation Work Plan to gain an understanding of the planned contents for the ETR. Both of these activities should be performed prior to finalizing the validation plan. These checks must be performed during the preparation phase, in order to minimize the likelihood of schedule impacts while the evaluation is ongoing.

The ST for the evaluation must list all applicable assurance requirements and the Evaluation Work Plan should document how the evaluation analyses for each assurance requirement will be performed. The Validator should perform a simple mapping between the work packages listed in the Evaluation Work Plan and the assurance requirements in the ST to ensure consistency between the two documents.

The Validator should confirm that the planned ETR is appropriate for the evaluation and that it follows the latest ETR templates from the Validation Body. Two ETR templates are available, one to be used for a TOE evaluation and the other to be used for a PP evaluation. A description of the ETRs is provided in Scheme Publication #4, *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Guidance to Common Criteria Testing Laboratories*. The latest releases of the ETR templates can be found at the CCEVS web site, URL: http://niap.nist.gov/cc-scheme/GuidanceDocs.html under the section “CCEVS Forms & Templates”.

The ETR is a CCTL record summarizing the results of the evaluation. The Validator should review the CCTL plans for preparing the ETR from the evaluation activities and understand what reporting information is planned to be included in the final ETR. The Validator should ensure that the planned ETR includes sections for reporting evaluation results of all assurance components for the evaluation. The planned ETR should be specifying the evaluation analysis, and the evaluation verdict with supporting rationale for each assurance component that constitutes an activity for the ST or PP.

The Validator must understand the planned CCTL reporting style for each assurance component in the ETR for planning validation activities in the validation plan. For example, if the reporting on evaluation of an assurance component is expected to provide sufficient details to enable the Validator to determine that evaluation analysis was complete and met requirements of the CEM, then simply planning to assess the evaluation results recorded in the ETR should be sufficient. If on the other hand, the

reporting on an assurance component is expected to provide insufficient information in the ETR to enable the Validator to determine complete and consistent application of the CEM, then the Validator should consider incorporating validation activities into the validation plan such as reviewing evaluation work records for specific work units.

4.1.4 CCTL Evaluation Procedures

CCTL evaluation procedure reviews can occur at several points during the validation process. During the preparation phase, the Validator must perform an initial evaluation procedure review to determine if all required procedures are available. This review gives the Validator insight into the methods that the evaluation team will use in conducting the evaluation. Based on the evaluation procedures, the Validator can plan the validation activities that are appropriate and plan the timing of the validation activities.

One of the Validator's first steps after reviewing the CCTL's work packages should be assessment of the CCTL evaluation procedures that apply in the evaluation. The CCTL should identify currently documented procedures to be used in the evaluation for the work packages identified. The CCTL should also identify any procedures expected to be used that have not yet been documented, or that will be developed during the evaluation.

The Validator should conduct a preliminary review of the existing documented procedures and use this information in determining what validation activities are needed in the validation plan. For an evaluation procedure that appears to be reasonably complete no further Validator review need be initially planned. If a procedure for a work unit appears to be incomplete or is undocumented, or is addressing a technology area where little experience is available, the Validator should plan a detailed review of these procedures in the conduct phase.

The Validator is not required to perform a detail review of all documented evaluation procedures; however, the Validator must understand all evaluation methods that the CCTL will use in the evaluation. The Validator should plan for a detail review of selected CCTL procedures as needed. The Validator should consider doing a detail review of evaluation procedures when a more thorough understanding of a particular CCTL evaluation approach is needed.

4.1.5 CC, CEM and CCEVS Policy Interpretations

The Validator should conduct an initial review of CC, CEM and CCEVS policy interpretations as early as possible in the evaluation process. The primary purpose of an initial interpretations review is to help identify interpretations applicable to the evaluation.

4.2 Meetings

Two validation meetings take place during the preparation phase. These two meetings are the Evaluation Acceptance Kick-off and the Procedures and Records Orientation. The purpose of validation meetings is to enable the Validator to discuss with the sponsor and CCTL validation requirements and to plan validation activities.

Either at the Evaluation Acceptance Kick-off meeting or during the CCTL Procedures and Records orientation the Validator and CCTL should reach agreement on how communications of sensitive information will be handled between them. Consideration should be given to (unencrypted) e-mail, e-mail with encryption, on-site-only access to evaluation evidence, surface mail packaging, etc.

4.2.1 Evaluation Acceptance Kick-off Meeting (Mandatory)

Within 8 business days of assignment and receipt of the Evaluation Acceptance Package, the Validator should schedule an Evaluation Acceptance Kick-off Meeting. The *kick-off meeting* provides an opportunity for all parties involved in the evaluation and validation to meet and agree on expectations. The purpose of the Evaluation Acceptance Kick-Off meeting is to introduce the CCTL, Validation Body and Sponsor representatives, and to achieve an understanding among the participants of each organization's roles, expectations, and plans for the evaluation. Technical details of the product or the evaluation criteria to be used should not be discussed at the meeting.

The Validator will conduct the kick-off meeting. The lead evaluator, lead Validator, sponsor representative, Validation Body management, and others as appropriate, should participate in the meeting. If the Validation Body management is unavailable for the meeting, the Validator serves as the Validation Body management representative.

Once this meeting has occurred and all parties are in agreement, the Validation Body, CCTL, and Sponsor sign an *Evaluation Acceptance and Non-Disclosure Agreement* affirming that the evaluation has been officially accepted by the Validation Body for validation processing and evaluation activities may proceed.[4]

A sample *Evaluation Acceptance Kick-off Meeting Agenda* and an electronic copy of the *Evaluation Acceptance and Non-Disclosure Agreement* are available through the CCEVS web site at URL: http://niap.nist.gov/cc-scheme/GuidanceDocs.html under "CCEVS Forms & Templates".

[4] If a CCTL begins an evaluation before obtaining official acceptance for validation processing by the Validation Body, may require some evaluation process steps be re-started in order for the Validator(s) to perform their functions.

4.2.2 Procedures and Records Orientation Meeting (Optional)

A *Procedures and Records Orientation* should be scheduled so the Validator has a full understanding of the CCTL evaluation procedures and record keeping to be used for the evaluation. Whether through a meeting, documentation review, or informal discussions with the evaluation team, the Validator must understand the CCTL's evaluation approach, specifically focusing on the procedures and records to be used for the evaluation. The Validator must obtain information about the types of records that will be maintained, the storage and availability of the records, how proprietary data is to be handled and transmitted, and the timing and frequency of record generation by the evaluation team. The Validator should focus on determining how the records to be generated and maintained by the evaluation team will be used to perform the validation. Because evaluation records play such a vital role in the performance of the validation, the procedures and records information obtained by the Validator will have a direct impact on the validation plan. If the Validator will have access to detailed and current evaluation records throughout the validation, the validation plan approach should be largely focused on records review. However, if the evaluation records will be minimal or difficult for the Validator to access, this must be reflected in the validation plan.

4.3 Documents

4.3.1 Validation Plan

The Validation Plan is developed from information in the ST or PP, Evaluation Work Plan, the Validator's understanding of the CCTL's evaluation procedures that will be used, and records that will be kept. See Annex D for a Validation Plan worked example. The validation activities described in Sections 4, 5 and 6 of this document, and the Validator guidance offered in Annex C provide the foundation for what should be addressed in the Validation Plan. The plan should take into account the CCTL history of performance. The Validation Plan will outline the various validation activities and validation milestones. The Lead Validator then presents the completed plan to the Chief Validator or designee for concurrence. The Validation Plan is due to the Chief Validator or designee no later than 8 business days after the Procedures and Records Orientation Meeting. If the Validator chooses not to have a Procedures and Records Orientation Meeting the Validation Plan is due 8 business days after the Evaluation Acceptance Kick-off Meeting. Following approval of the Validation Plan by the Chief Validator the Validator will forward a copy of the Validation Plan to the CCTL and the Records Manager.

4.3.2 Work Package Assessment Table

To support execution of the Validation Plan the Validator should develop a Work Package Assessment Table containing a list of work units associated with the work packages. The first step in developing this table is for the Validator to confirm that the

work packages listed in the CCTL's Evaluation Work Plan are consistent with the assurance requirements of the security target [or protection profile]. This should be a simple mapping. Next the Validator should develop a table containing cells for each work package, work unit, verdict, and rationale for verdict. The list of these work packages and associated work units should be the same as those listed in the Evaluation Work Plan. The table should also include columns for verdict and the rationale that supports the verdict, which will be filled in during the course of the evaluation. Section 5.2.5 provides guidance on how this table will be used throughout validation of the evaluation results.

4.3.3 Memorandum for Record

The Validator or designee shall generate a Memorandum for Record (MR) to document activities. At a minimum a MR should be used to document minutes of all meetings and/or technical exchanges, reviews conducted, and all forms of guidance provided to the CCTL. Annex D contains the format and content requirements for a MR.

4.3.4 Evaluation Acceptance Agreement

At the conclusion of the Evaluation Acceptance Kick-off Meeting the Validation Body, CCTL, and Sponsor sign an *Evaluation Acceptance and Non-Disclosure Agreement* affirming that the evaluation has been officially accepted by the Validation Body for validation processing. An electronic copy of the *Evaluation Acceptance and Non-Disclosure* Agreement is available through the CCEVS web site at URL: http://niap.nist.gov/cc-scheme/GuidanceDocs.html under "CCEVS Forms & Templates". The Validator is responsible for coordinating with the Records Manager for the preparation of the agreement, obtaining the necessary signatures and returning the completed agreement to the Records Manager.

4.3.5 Approval to List Evaluations in Progress

Each sponsor of an evaluation should sign a *Sponsor's Approval to list Products that are "In Evaluation"*, CCEVS Form F8001, stating whether the product or PP may be publicly posted as being "In Evaluation" on the CCEVS web site. An electronic copy of CCEVS Form F8001is available through the CCEVS web site at URL: http://niap.nist.gov/cc-scheme/GuidanceDocs.html under "CCEVS Forms & Templates". The Validator is responsible for coordinating with the Records Manager the preparation of CCEVS Form F8001, obtaining the necessary signatures and returning the completed form to the Records Manager.

5 Conduct Phase

After an evaluation has been officially accepted by the Validation Body for validation processing, the conduct phase commences. The CCTL will conduct all evaluation activities in accordance with the CC and CEM, the CCTL evaluation procedures, the Evaluation Work Plan, and CCEVS processes. The Validator should concurrently monitor CCTL activities, perform and document validation activities in accordance with the Validation Plan, prepare and submit validation status reports, coordinate all CCTL-generated Observation Reports (ORs) submitted to the Validation Body, and provide support to the CCTL as needed. The Validator should update the Validation Plan as necessary to keep current with changes in evaluation plans and activities. The Validator should perform work commensurate with the validation activities described in the Validation Plan.

Upon completion of all evaluation activities, the CCTL prepares and submits an ETR to the Validator. The final ETR is provided in two forms: a) a complete ETR (including proprietary and/or sensitive information), and b) an abridged ETR (complete report excluding proprietary and/or sensitive information). In addition, the CCTL provides the Validator with the final ST or PP, all evaluation Observation Reports (ORs) along with corresponding Observation Decisions (ODs), and a draft Validated Products List Entry.

The Validator reviews the final ETR and the other submissions to determine accuracy and completeness. The Validator reviews the draft VPL entry, and works with the Validation Body, the CCTL, and the Sponsor of the evaluation to produce a VPL entry suitable for public posting.

The conduct phase officially ends when the Validator accepts the final versions of the ST or PP and ETR, all evaluation ORs along with corresponding ODs, and a draft Validated Products List (VPL) Entry. The sections below identify the validation activities used, and how they are applied to this phase of the validation.

5.1 Evaluation Monitoring

Evaluation monitoring activities are those activities that offer confidence that evaluations are being performed with consistency and quality according to CCEVS requirements. The approach for this set of activities is for the Validator to gain confidence by using two primary methods: the ‘quality process check’ and the ‘evaluation activity assessment’. The quality process check offers confidence the CCTL is identifying the correct work units and is defining the appropriate procedures (i.e., work instructions) for performing the work units. The evaluation activity assessment offers confidence that the evaluation results are technically sound and the CCTL consistently applied the CC and the CEM. The two validation methods work together to verify the evaluation results. Much of the information in assessing evaluation activity is gathered by reviewing the technical output and records of the evaluation. As CCTLs become more mature and demonstrate more experience, such confidence could be gathered more from quality process check, striking

more of a balance between process and technical output review. Various validation activities used for the conduct phase of evaluation described herein enable quality process checking and evaluation activity assessment.

Another aspect of evaluation monitoring is activities that offer confidence that evaluations are performed impartially and adhere to the principles of operation documented in CCEVS publications and notices, and the CEM. For example, evaluations that do not appear to involve a separation between the developer of evidence and the evaluator of that evidence violates the principle that product or PP evaluations should be conducted independently and impartially. Validator communication and interactions with the CCTL, Validator observance of CCTL operating activities, and Validator review of CCTL developed evaluation materials are validation activities that should offer confidence that CEM and CCEVS principles of operation are being followed in evaluations. If the Validator feels that an evaluation is not being conducted in accordance with CCEVS requirements, the Validator should raise the issue with the CCTL and Validation Body management, and document in validation records the issue, the actions taken, and the resolution.

5.2 Reviews

5.2.1 Security Target

The Validator should become extremely familiar with the ST and clearly understand the scope of the TOE and the set of security requirements taking note of tailoring of the CC requirements. The Validator must review the ST to ensure that CC interpretations are addressed and that the ST can serve as an adequate specification for product evaluation.

For the conduct phase the Validator shall conduct a detailed review of the ST. The goal is to see if there are misunderstandings or glaring errors in the ST that would affect the TOE evaluation. Some items to look for in this review include:

- Does the TOE Environment appear sound? Are the assumptions appropriate, or should they be stated as threats? Do the threat statements contain a threat agent, asset that is threatened, and the attack? Does the attack contain the method of attack and the result of the attack?

- Are the objectives consistent with respect to the assumptions, threats, and Organizational Security Policies? Does the objective rationale take the right approach in describing how the objectives counter or mitigate the threats?

- Are the requirements section largely complete, with all operations (especially assignment, refinement, and iteration) performed? Do the operations appear to be performed correctly? Do application notes levy requirements that are not allowed?

- Does the TOE Security Specification describe security functions? Does it describe how the security functions "meet" the requirements in the TOE requirements section? Does the TOE Security Specification describe assurance measures, and how those measures "meet" the "D" (developers action) and "C" (content and presentation) elements of the assurance requirements.

- If the ST claims that the TOE conforms to one or more PPs, does the ST provide an explanation, justification and supporting material of this claim. Does the ST clearly reference the PP? Does the ST provide a clear PP tailoring statement, and, if applicable, a PP additions statement?

5.2.2 Protection Profile

The Validator should become extremely familiar with the PP and clearly understand the scope of the TOE and the set of security requirements taking note of tailoring of the CC requirements. The Validator must review the PP to ensure that CC interpretations are addressed, and that the PP can serve as a sound specification for a class of products from which STs can be specified and TOEs evaluated.

In addition to the general review performed in the preparation phase, the Validator shall perform a more detail review of the PP. The goal is to see if there are misunderstandings or glaring errors in the PP that would inhibit it from serving as a sound set of security requirements for STs and TOE evaluations. Some items to look for in this assessment include:

- Does the TOE Environment appear sound? Are the assumptions appropriate, or should they be stated as threats? Do the threat statements contain a threat agent, asset that is threatened, and the attack? Does the attack contain the method of attack and the result of the attack?

- Are the objectives consistent with respect to the assumptions, threats, and Organizational Security Policies? Does the objective rationale take the right approach in describing how the objectives counter or mitigate the threats?

- Are the requirements section largely complete, with all operations (especially assignment, refinement, and iteration) performed? Do the operations appear to be performed correctly? Do application notes levy requirements that are not allowed?

- Does the PP describe implementation-independent sets of security requirements adequate for a category of TOEs and contain a statement of the security problem that a compliant product is intended to solve?

5.2.3 CC, CEM and CCEVS Policy Interpretations

In evaluation of a TOE or PP the evaluation-applicable CC, CEM, and CCEVS Policy interpretations must be correctly applied for the evaluation. The CCTL is responsible for identifying and using all applicable interpretations in evaluation. Section 8.2.2, Applying Interpretations, provides guidance on what interpretations should be applied. The Validator must confirm that all applicable interpretations are appropriately applied. The Validator should keep the evaluation team informed throughout the evaluation of any applicable and pending interpretation actions that may effect the evaluation.

5.2.4 CCTL Evaluation Procedures

The purpose for reviewing CCTL evaluation procedures during the conduct phase is to determine that the CCTL is following acceptable evaluation procedures in conducting the evaluation. In making this determination the Validator must review selected CCTL evaluation procedures as planned or needed. The Validator must determine that the evaluation procedures do not conflict with the CC, CEM, CCEVS, or industry-agreed evaluation processes for the technology being evaluated, and are appropriate for the product or PP being evaluated. Annex C provides some guidance the Validator should draw upon in determining if the CCTL procedures are appropriate.

If a complete set of procedures for the evaluation was not documented prior to the start of the conduct phase, the Validator must review the new or modified procedures when completed. The Validator must become familiar enough with the CCTL evaluation procedures to understand the evaluation approach and how verdicts are determined. This understanding should be detailed enough to allow the Validator to determine if the procedures were followed by the evaluation team in conducting the evaluation. This can be accomplished by reviewing the written evaluation procedures, or if needed through observation and/or discussion with the evaluation team.

If the CCTL has proposed a procedure for a unique aspect of a vendor's evidence, the Validator may need to review the evidence to determine if the procedure covers relevant aspects for the requirement. For example, if a CCTL has a "API review procedure" for ADV_FSP work units and a vendor presents a unique network interface that requires the CCTL to develop a new procedure, the Validator may need to check the elements of the procedure (e.g., examination of effects, error messages, and exceptions) against the elements presented in a sample of the network interface documentation to ensure 1) that all elements of the ADV_FSP work units are being addressed by the procedure, and 2) the evidence being required is consistent with evaluations being performed by other CCTLs.

5.2.5 Evaluation Work Package (EWP) Records

The CCTL's quality system evaluation records (work records and ETR) are the primary source of validation information for confirming correct and complete evaluation analysis. These records provide the information for confirming that the evaluation was performed in an acceptable manner.

To support the ETR review and supplement understanding of the evaluation analysis and verdict rationale, the Validator should review CCTL evaluation work records. The general model is that the Validator reviews the CCTL records related to the evaluation activity to be assessed. The Validator then analyzes the evaluators' analysis of the evidence, and provides feedback to the evaluators if necessary. The Validator could gain the necessary information from informal meetings with the evaluation team, from informal notes and records kept by the evaluation team, from work package documentation, or from draft ETR sections. The Validator should make every attempt to perform the records review throughout the course of the evaluation in order to mitigate the risk of unexpected technical issues at the end of the evaluation. In some cases the Validator may need to supplement records review by reviewing evaluation evidence to verify the CCTLs' analysis. The Validator should not perform an evaluation on a piece of evidence, but review the evaluation evidence for obtaining a better understanding of the analysis performed or for clarifying information in CCTL records. The extent of the evidence review depends on the EAL (higher EALs include more evaluation evidence), the detail provided in CCTL records, the Validator's experience with the CCTL personnel, and interactions with team members. The goal is to spot-check the technical accuracy of the CCTL's analysis, to gain confidence that the CCTL is following their procedures, and that they are accurately documenting the results.

The Validator shall review the evaluation records for each work package to determine the extent of compliance. The Validator's assessment is documented in the verdict and rationale columns of the Work Package Assessment Table (See Section 4.3.2).

The following are possible verdicts:

> **Compliant** - The documented activities fully satisfy the requirements of the CC and CEM.
> **Satisfactory** - The documented activities appear to satisfy the requirements of the CC and CEM, but the Validator needed additional knowledge or information beyond that provided by the evaluation record.
> **Deficient** - The documented activities do not satisfy compliance with the CC and CEM or the record of those activities that are inadequate to demonstrate compliance.

A verdict of "Satisfactory" and "Deficient" requires additional action. If the evaluation record did not provide the knowledge or information needed to determine if an activity

satisfies a CEM requirement, the issue should be documented and tracked until the CCTL resolves the problem. Annex C provides validation guidance for some CEM work units the Validator can use for determining if the recorded evaluation results are acceptable.

For those work units that have yet to be completed, the verdict should be entered as "Not Completed". The verdict and rationale columns can then be used as both feedback to the CCTL and progress status to the Validation Body.

The Validator should use the CCTL's evaluation records as needed when performing the final ETR review. The records should be assessed to provide greater details about the results of the evaluation analyses.

5.2.6 Evaluation Technical Report (ETR)

The ETR is expected to provide a comprehensive summary of the TOE or PP evaluation and include a description of how the evaluation was conducted, and the results of the evaluation. In reviewing the ETR, the Validator may review evaluation records to verify that the verdict given for a particular Evaluator Action Element or work unit is consistent with the evidence provided. In cases where the Validator determines that the information in the ETR and CCTL work record are insufficient, the Validator may need to review evaluation evidence to confirm the evaluation analysis and verdict. If evaluation evidence is reviewed, the Validator should then describe to the CCTL the type of information that is expected to be reported in the ETR or evaluation record using the evidence to illustrate the Validator's points.

5.2.6.1 Incrementally Developed ETR

To identify potential validation issues as early as possible the Validator should review draft ETR sections when provided by the CCTL during the conduct phase. An incremental ETR delivery schedule will help to mitigate the risk of unexpected technical issues arising at the end of the evaluation.

The results from Validator review of draft ETR sections can serve as a driver for determining if additional validation activities are needed. If the draft ETR section provides a clear and complete statement of the evaluation method used, the evaluation analysis, verdict obtained, and the rationale for the verdict then there is no need for performing additional validation activities for that section. If the draft ETR section did not provide a clear and complete statement, then the Validator should conduct additional validation activities such as review CCTL supporting records, interact with evaluation team to clarify evaluation reporting, etc.

5.2.6.2 Final Completed ETR

The Validator is required to review and accept the final ETR before recommending that the TOE/PP be awarded a certificate by the CCEVS. The final ETR review should be comprehensive and the Validator must ensure that the information presented is complete, and that is consistent with the analysis that was performed by the evaluation team. The rigor applied to the ETR review should be based on the assurance level.

In reviewing the ETR, the Validator shall review each verdict and associated rationale described by the CCTL in the ETR. The Validator shall ensure that enough information is provided by the CCTL in the rationale to support their verdict. The CEM allows verdicts and rationale to be presented at the assurance component level or the work unit level. However, the evaluation team could supply verdicts and rationale at the CEM work unit level. If the evaluation team chooses to provide verdicts and rationale at the assurance component level, the rationale must address all the CEM work units that fall within the given assurance component.

The Validator should be looking for evidence in the rationale that the CEM work units were properly performed. A rationale that simply repeats or is a paraphrase of the CEM work unit is unacceptable. The CEM states: "The rationale justifies the verdict using the CC, the CEM, any interpretation and the evaluation evidence examined and show how the evaluation evidence does or does not meet each aspect of the criteria. It contains a description of the work performed, the method used, and any derivation of the results".

As an example, consider the CEM work unit ADV_FSP.1-2. This work unit requires the evaluator to examine the functional specification to determine that it is internally consistent. It is insufficient for the evaluator's rationale to state that the functional specification had been thoroughly reviewed and that no inconsistencies had been found. The level of detail in an adequate rationale could be something like the following:

> "The evaluation team developed a matrix that identified every interface in the functional specification in the first column. The characteristics for the team's notion of consistency where then added as subsequent columns. These characteristics included the functional description of the interface, parameters passed to the interface, and the error messages generated by the interface. The functional specification was then reviewed to ensure that these characteristics were consistent with one another for each interface. For example, if an error message was identified for an interface that stated "access is denied" and the interface only takes a file descriptor as a parameter, which suggests the file has already been opened and access checks had been performed, that would lead us to believe there was an inconsistency. Or if an interface description discusses traversing a pathname supplied by the user and a file descriptor rather than a pathname is supplied as a parameter this would be considered an inconsistency.

During the course of our analysis the team discovered twelve inconsistencies in our first review and these inconsistencies are identified in record <record-identifier>, which contains the matrix and a pointer to the comments the team provided to the sponsor. The sponsor addressed our comments and the inconsistencies have been addressed. Record <record-identifier> contains the updated matrix, a pointer to the sponsor's response and a pointer to the updated functional specification.

The team has examined every interface in version X of the functional specification and found that the characteristics we identified for consistency were consistently described for each interface."

The Validator should also ensure that any ORs/ODs are appropriately included in the evaluation and described in the ETR. The Validator shall ensure that there are no inconsistencies between the ETR and the ST or PP. The Validator shall use information and knowledge obtained in performing the validation activities listed in Validation Plan to ensure that the CCTL has arrived at an appropriate verdict for the analysis presented for work units and Evaluator Action Elements selected.

The Validator should work with CCTL personnel to address any issues that they find in the review. These issues could range from factual errors in the ETR, to omissions, to areas that are unclear to the Validator.

5.3 Meetings

Meetings with the evaluation team should be held when needed for supplementing the Validator's understanding of the product or PP evaluation.

Meetings between the Validator and the evaluation team should be identified in advance, when possible, and included in the Validation Plan. Depending upon the information to be discussed, meetings may involve presentations, hands-on work on the system under evaluation, review of evaluation evidence (i.e., work unit analysis), or question and answer sessions. The style and format of validation meetings with the evaluation team will be agreed upon prior to the meeting. These meetings are not intended to place undue burden on the CCTL or sponsor, but will require some preparation by all those involved, in order to allow for worthwhile technical discussions to occur.

When ATE_IND is included in the ST, a meeting may be scheduled before independent testing. However, if ATE_DPT or ATE_COV is in the ST, this meeting should be scheduled after the coverage and depth of the developer's tests has been verified and any required functional testing by the developer has been evaluated. Discussions for this meeting should focus on the evaluation team's plans for the independent testing to be performed and the results of the analysis of the developer's test suite. Documentation will include the evaluation team's test analysis results and the team's test subset, for independent testing.

When components from AVA_VLA are included in the ST, an additional meeting may be scheduled after testing and evaluation of the vulnerability assessment. Discussions at this meeting will demonstrate the adequacy of the testing and vulnerability assessment efforts. Documentation to be presented at the meeting includes the evaluation team test documentation, the verdict for the activity, verdicts for the vulnerability assessment, and evaluation of the vulnerability analysis activities, including supporting documentation. Other items addressed, depending on ST contents, are the evaluation evidence for the evaluation of misuse and the strength of TOE security functions.

When ADV components are included in the ST, the Validator should gain insight into the evaluation team's activities in applying the components. This is important to do early, possibly before any ETR sections have been generated, because problems not caught at an early stage may have a profound impact on the schedule if left to the end.

Participating in a team meeting discussing the team's analysis will give the Validator insight into the team's application of the CC and CEM. For the meeting, the Validator should have sufficient insight into the evidence that the team will be discussing so that they can assess the team's application of the CC and CEM to the evidence. Again, the Validator should not perform an evaluation of the evidence, but they are expected to have enough familiarity so that they can understand the issues the team is discussing and thus gain confidence in the team's analysis methods.

5.4 Observe/Witness

5.4.1 Observe CCTL Evaluation Team Meetings

The Validator may observe selected evaluation team meetings, if deemed necessary, to supplement Validator understanding of the evaluation. The Validator should arrange in advance with the CCTL to attend the evaluation team meeting as an observer. Observation of evaluation team meetings provides the Validator with an opportunity to hear the technical discussions and to obtain insight about the type and level of analysis that the evaluation team is performing.

Factors that a Validator must take into account when determining whether to attend evaluation team meetings include the EAL of the evaluation, material written by the evaluation team (e.g., records) prior to the meeting, and team policies with respect to meetings. For lower EALs, the Validator may choose not to attend meetings and instead focus on review of the ETR sections and records, since these evaluations will typically be of short duration. For higher EALs, where it is vital to identify issues at the outset, it is more common that teams will hold meetings to discuss a certain aspect of the evaluation without having prepared any records. In these cases, the Validator should base attendance on the perceived impact the discussion will have on the evaluation (for example, a discussion of the developer's proposed format for subsystem documentation in satisfaction of the ADV_HLD components). It may also be the case that the team

conducts all of their meetings "electronically", sending comments back and forth through e-mail, for instance. In these cases, the Validator may wish to examine the e-mail messages to gain confidence in the evaluation team's activities. In summary, if the Validator has questions about any aspect of the evaluation, attendance at some team meetings are a way to fill in the gaps in the written information provided by the evaluation team. Another consideration in deciding to attend an evaluation team meeting is the type of evaluation activity being performed. For example, the Validator should make an effort to attend at least one evaluation team meeting held in preparation for testing.

5.4.2 Witness CCTL Testing Activities

If a TOE is being evaluated, product testing is generally a good activity for the Validator to witness.

Before witnessing testing, the Validator should determine that the evaluators have a comprehensive understanding of the test suite. The evaluation team should understand the vendor test suite; agree with the expected test results as documented in the developer delivered test documentation; review the developer vulnerability analysis; and know exactly what functions are NOT tested (if any) by the developer test suite. The Validator can accomplish this by reviewing a Test Report (draft ETR section) generated by the evaluators, or by meeting with the evaluation team.

During testing, the Validator should determine that the evaluators are using and confirming the AGD related documentation (user guide and administrative guidance), and ADO related documentation.

The Validator may witness some amount of testing performed by the evaluators. The subset of testing should include some of the developer tests as well as some of the independent tests. The Validator should confirm that the test results witnessed were those reported by the developer as actual test results and listed in the test documentation as expected test results (for the vendor tests). The Validator should also witness work associated with installing the TOE (ADO_IGS).

5.5 Documents

5.5.1 Memorandum for Record

The Validator or designee should generate a Memorandum for Record (MR) to document validation activities. At a minimum a MR should be used to document minutes of all meetings and/or technical exchanges, reviews conducted, and all forms of guidance provided to the CCTL. Annex D contains the format and content requirements for a MR.

5.5.2 Monthly Summary Reports

The Validator shall document in a monthly report the project accomplishments, status and any technical or management issues. Monthly Summary Reports are to be submitted by the 5th day of each month for the preceding month. Annex D provides the format and topics for Monthly Summary Reports. Monthly Summary Reports should be forwarded to the ccevs-staff@nist.gov and ccevs-records@nist.gov mail list.

5.5.3 Work Package Assessment Table

Upon completing the work package assessment table for a TOE, the Validator must make a recommendation as to whether the laboratory has satisfied the work packages. This recommendation is based on the overall state of this table. If the verdicts are all compliant or satisfactory, the recommendation should be that the work packages have been completed. If there are any deficiencies, the recommendation should be that the work packages have not been completed. The Validator's recommendation is documented in a Memorandum for Record (MR) with the completed Work Package Assessment Table as an attachment.

5.5.4 Observation Reports/Observation Decisions

The Validator is responsible for ensuring that final Observation Reports (ORs) and Observation Decisions (ODs) are submitted to ccevs-records@nist.gov mail list. The process for submission and handling CCEVS ORs can be found in Section 8.4.1.1 and 8.4.1.2 respectively. The format for the OR/OD is located in Annex D.

(This page intentionally left blank)

6 Conclusion Phase

After Validator acceptance of the final ETR, they will use the ETR in conjunction with the other CCTL-provided information to produce a Validation Report. When the Validation Report is completed the Validator will submit the report to the Chief Validator for review. Upon Chief Validator concurrence with the VR the Validator will coordinate with the Records Manager to submit the VR, ST or PP, draft Validated Products List Entry, and draft Common Criteria certificate information to the CCTL for Sponsor and CCTL review. The CCTL and Sponsor review is to confirm that this material 1) contains no company proprietary information, 2) does not contain technical inaccuracies and 3) is approved for public distribution by the NIAP CCEVS. The Validator will review and coordinate with the Records Manager changes requested by the CCTL or Sponsor to the VR, ST or PP, Common Criteria Certificate information and VPL entry.

Upon notification of approval from the Sponsor and the CCTL to publicly post the VR, ST or PP and VPL entry, the Validator will provide a final recommendation to the Chief Validator for concurrence and for presentation to the Director of the Validation Body.

Using the final recommendation, the Director of the Validation Body will make the decision on whether to issue a Common Criteria Certificate. If a certificate is to be issued, then the Validation Body will arrange for preparation and signature of a Common Criteria Certificate, and for posting the validated IT product or PP to the NIAP Validated Products List or Protection Profile Registry as appropriate. The Validation Body will notify the other CCRA-recognized validation/certification bodies accordingly. If a certificate cannot be issued the Director of the Validation Body will coordinate with the Validator and notify the CCTL and Sponsor of the unsuccessful completion of the evaluation and provide rationale for this decision.

The Validator is responsible for coordinating completion of the VPL entry and Common Criteria Certificate information form with the Records Manager. In addition the Validator must provide the final Validation Report and ST or PP in electronic form to the Records Manager for posting to the CCEVS web site. The final versions of these documents should be submitted to the Validation Body in a text editable format.

Whether the validation was successful or not, the Lead Validator is responsible for ensuring that all validation records and reports are turned over to the CCEVS Records Manager for archiving.

The conclusion phase ends with the delivery of a Validator's Lessons Learn Report and the holding of a validation *post-mortem* meeting for assessing what can be done to improve the effectiveness and efficiency of both CCEVS and CCTL procedures.

6.1 Documents

6.1.1 Validation Report

After a detailed review and acceptance of the ETR, the Validator will use the ETR together with the other CCTL provided information and Validator generated records to produce a Validation Report. The format for the *Validation Report* is available in Annex D.

6.1.2 Validated Products List (VPL) Entry

One of the deliverables from the CCTL is a draft VPL entry for the Validated Products List or the Protection Profile Registry. The Validator uses this information to prepare the final VPL entry. The format for the VPL entry can be found at the CCEVS web site at URL: http://niap.nist.gov/cc-scheme/GuidanceDocs.html under the section "CCEVS Forms & Templates".

6.1.3 Draft CC Certificate Information

From information found on the VPL entry and Validation Report, the Validator prepares the information needed for preparing the Common Criteria Certificate. The format for providing the Common Criteria Certificate Information, form CCEVS T6003, is available in Annex D.

6.1.4 Vendor/CCTL Approval for Release of Validation Information

The Validation Report, ST or PP and draft Validated Products List Entry will concurrently be submitted to the CCTL and Sponsor for accuracy review and release approval. See CCEVS web site at URL: http://niap.nist.gov/cc-scheme/GuidanceDocs.html under "CCEVS Forms & Templates" for an electronic copy of the latest version of CCEVS Form F8002, *Sponsor/CCTL Approval for Release of Information*. The Validator is responsible for coordinating with the Records Manager for preparation, signing, and completion of this form.

6.1.5 Validator Recommendation

Upon notification that approval from the sponsor and the CCTL to release the VR, ST or PP and certificate information has been received, the Validator will provide a final recommendation to the Chief Validator for concurrence and presentation to the Director of the Validation Body. This recommendation will be documented in the form of a

Memorandum for Record (MR). The Validation Recommendation format, form CCEVS T6002, can be found in Annex D.

6.1.6 Lessons Learned Report

Upon conclusion of the validation the Validator will prepare a report of lessons learned about the evaluation/validation project. The purpose of the assessment is to give feedback to Validation Body management to provide the opportunity for improving the evaluation and validation process. The lessons learned report should be documented and include information on both successful and troublesome events, and recommendations for improving the process. The lessons learned report is submitted to the Chief Validator via the ccevs-records@nist.gov mail list. Feedback to the CCTL shall be coordinated through Validation Body management.

6.1.7 Monthly Summary Reports

A Monthly Summary Report will be generated to document the status of the conclusion phase activities until all validation processes have been completed.

6.2 Validation *Post-Mortem* Meeting

The Validator will participate in a *post-mortem* meeting with the Validation Body during the conclusion phase. This meeting will be held to review the validation project and the Lessons Learned Report with the Validator in order to promote continuous improvement of the Validation Body and the CCTL procedures. The focus of the meeting will be to discuss areas in the evaluation and validation process that were both effective and ineffective in the project, and to obtain Validator recommendations for improving the process in future validations. Meeting topics should include what the Validation Body should do to help improve the performance and capability applicable to all CCTLs, what specific procedures, training, process or technical guidance should be developed for Validators or CCTLs, and what changes or clarifications are needed in the CC standards. Additionally, the Validation Body, as it deems necessary, will provide the Validator with specific questions/issues to be addressed. If warranted, appropriate portions of this feedback will be provided to NVLAP for use during CCTL assessments.

(This page intentionally left blank)

7 CCEVS Record System Requirements

To comply with the CCEVS Quality System the Validator must keep records of their work. The purpose of the validation records is to provide a written history of what activities a Validator performed, including what guidance was provided to the evaluation team. If a Validator is unable to serve until the completion of the evaluation, another Validator can take over and know what has been accomplished, as well as what guidance has been provided to the evaluation team.

7.1 Validation Records

The Validator is required to document the validation efforts in validation records and eventually a Validation Report. The validation records will be used as input when writing the Validation Report. The records will also be available to all Validators (as needed) and can be used as guidance to less experienced Validators, and will help ensure consistency among Validators.

In order to effectively capture the activities of the Validator and to ensure streamlined retrieval of records, six record categories have been identified. The Validator must determine the category to which the record belongs and assign a record identifier accordingly. The record identifier will be discussed further in section 7.2, Record Identifiers and Indexing. The six categories are:

1. Validation Plan (VP)
2. Memorandum For Record (MR)
3. Monthly Summary Reports (MSR)
4. Validation Report (VR)
5. Validated Products List (VPL) Entry
6. Observation Reports/Observation Decisions (OR/OD)

7.1.1 Validation Plan (VP)

This record is used to document the overall validation activities planned for the evaluation. Since the Validation Plan is tied to the Evaluation Work Plan the Validation Plan should be considered to be an evolving document. As changes are made to the Evaluation Work Plan (e.g., schedule changes, ST revisions, etc) the Validation Plan should be updated accordingly. The initial Validation Plan must be forwarded to the ccevs-staff@nist.gov mail list for Chief Validator approval. All VP revisions shall be forwarded to the ccevs-records@nist.gov mail list as they occur. See Annex D for Validation Plan format and content.

7.1.2 Memorandum For Record (MR)

A Memorandum for record (see Annex D for format) will be generated to document all of the following activities:

Meeting minutes,
Validator reviews of documentation,
Validator witnessing, monitoring & interaction with evaluation team,
Validator guidance/direction given to evaluation team,
Validator Pass/Fail Recommendation,
Work Package Assessment Table, and
Lessons Learned Report.

The format for the Validator Pass/Fail Recommendation, form CCEVS T6003, is provided in Annex D

MRs may include attachments as needed to complete the record.

The Validator has the option to file MRs with the Records Manager either on a monthly basis or at the end of the evaluation. Since MRs contains the details of validation work it will be used as the basis for Validator monthly summary reporting.

7.1.3 Monthly Summary Reports (MSR)

Throughout the course of the evaluation the Validator is required to report the status of the validation activities in Monthly Summary Reports. The purpose of the Monthly Summary Report is to summarize the monthly validation activities and status, and raise problematic issues of technical, operational or personal concern to the Validation Body. The Monthly Summary Report will be used to monitor project status against schedule, outstanding actions, as well as Validator accomplishments. The format for the *Monthly Summary Report* is provided in Annex D.

7.1.4 Validation Report (VR)

The Validation Report summarizes the results of the evaluation; the validation activities performed and contain information confirming that the verdict rendered by the evaluation team was complete and consistent with the facts presented. See Annex D for the Validation Report format. The VR is a publicly releasable document that will be posted to the NIAP CCEVS web site; therefore, it cannot contain any proprietary or protected information. Once the VR is written the Validator should coordinate with the Records Manager to obtain vendor and CCTL release approval, prior to forwarding the VR to the Validation Body management for final approval. The final VR should be submitted in a text editable format. The preferred text format is Microsoft Word.

7.1.5 Validated Products List (VPL) Entry

The Validated Products List Entry record provides information for preparation of the Common Criteria Certificate and for posting the information on the NIAP CCEVS Validated Products List. It should not contain any proprietary or protected information, and like the VR it will require a release approval by the CCTL and Sponsor.

7.2 Record Identifiers and Indexing

It is essential for record management purposes that the Validator maintains all files in an organized manner. Therefore, every record maintained by the Validator must contain a unique record identifier.

The record identifier shall be located at the top right hand portion of the page and should be present on each page of the document. This identifier has the following format: VIDxxxx-[activity category acronym]-[unique one-up numbering (four digits) with optional alpha character]. The VIDxxxx is the project Validation Identification (VID) number. The first value, noted as "xxxx", is a unique number assigned by CCEVS Records Manager at the start of the validation. The second value identifies the activity category (e.g., VP, MSR, MR, VR, VPL), and the last required value is a four-digit one up number, which is determined by the Lead Validator and is used to distinguish records in the evaluation. In the case of validation teams, the Lead Validator could assign numbers as needed, or could assign each validation team member a block of numbers that the team is responsible for using. If an activity requires one or more revision of the original record then an alpha character will be added to the unique one-up numbering to uniquely identify "versions" of the record. For example if a Validation Plan is updated over the course of an evaluation, the initial version of the plan would have a record ID of VIDxxxx-VP-nnnn each revision of the Validation Plan will be annotated with an alpha character added to the end of the record ID (i.e., VIDxxxx-VP-nnnna).

Validators should keep an index of validation records for reporting, as well as, retrieval purposes. This index can be used to cut and paste into the "Records Generated" section of the Monthly Summary Reports, and at the conclusion of the evaluation, it will serve as a check to be certain that all the records are turned over to the Records Manager at close out. This index should include record identifier, type of record, date and author, and brief subject of the record. A sample index is outlined below.

VIDxxxx Validation Identification Number – assigned by Records Manager

Record ID	Type	Date	Author	Subject
VID3000-MR-0001	word doc	01/01/01	John R. Validator	kick off mtg
VID3000-MR-0002	pdf	01/03/01	Jane S. Validator	orientation
VID3000-VP-0003	word doc	01/08/01	John R. Validator	VP Initial
VID3000-MSR-0004	ASCII text	02/05/01	Jane S. Validator	MSR Jan 2001
VID3000-MR-0005	word.rtf	02/06/01	John R. Validator	ATE mtg
VID3000-VP-0003a	word.doc	02/07/01	John R. Validator	VP update
VID3000-VP-0003b	word.doc	02/15/01	John R. Validator	VP update
VID3000-VR-0006	word.doc	05/02/01	John R. Validator	Validation rpt.
VID3000-MSR-0007	ASCII text	06/02/01	John R. Validator	MSR Jun 2001

7.3 Proprietary Information

The Validator is responsible for properly identifying and protecting any proprietary or sensitive information in their possession.

7.3.1 Validation Records

All validation records should be considered CCEVS VALIDATION PROPRIETARY and afforded appropriate protection. The statement CCEVS VALIDATION PROPRIETARY must appear BOLDED at the top and bottom of each page of the document. For electronic email the proprietary marking must appear at the start and end of the text.

7.3.2 Evaluation Evidence

The Validation Body will not archive sponsor supplied evaluation evidence as validation records. If in the course of performing validation activities the Validator takes possession of proprietary evaluation evidence, that evidence must be returned to the party who provided the evidence, or the evidence destroyed, as agreed by the provider.

To maintain an accounting of evaluation evidence, the Validator must maintain a separate log of all proprietary evaluation evidence received and include that log as part of the Monthly Summary Reports. As a minimum the log must include the date the evidence was received, a description of the evidence item, from whom the evidence was received, who has possession of the evidence, and the date and to whom the evidence was returned, or how destroyed, as appropriate.

7.4 Electronic Records

Validation records should be recorded in electronic form whenever possible and sent to the mail list ccevs-records@nist.gov. Validation records sent to the ccevs-records@nist.gov mail list should include in the subject line, the record identifier (if it is a single record) or the Validation ID number (if it is for multiple records), and short title of the company and product name. Each attachment should be saved and titled with the record identifier as the name of the document. . For example:

1) For a single record:
To: ccevs-records@nist.gov
Subj: VIDxxxx-VP-nnnn, Company A, Product B

2) For multiple records:
To: ccevs-records@nist.gov
Subj: VIDxxxx, Date, Company A, Product B

7.5 Hardcopy Records

All hardcopy files should be organized, properly labeled with record identifiers and sent to:

NIAP CCEVS c/o Data/Records
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

7.6 Close Out of Validation Records

Official validation records must be closed out and transferred to the Records Manager within 30 days of the Validator delivery of the final validation report and VPL entry. Electronic and/or paper records shall be transferred along with an overall index of records for that evaluation. The Validator has the option to submit validation records to the Records Manager on a monthly basis to preclude a large delivery at the conclusion of the evaluation.

(This page intentionally left blank)

8 Validation Support Mechanisms

Support mechanisms available to the Validator in performing the assigned duties include, but are not limited to, other CCEVS technical resources, interpretations and policies, NVLAP or CCEVS remedial actions, the resolution process for evaluation issues, and CCEVS communication mechanisms.

8.1 Technical Support

The Chief Validator and senior members of the Validation Body are available to provide technical support to the Validator as needed. The Validator can request the Chief Validator's input prior to rendering guidance to the evaluation team. Some evaluations may require more support from senior members of the Validation Body than others. The level of Chief Validator and senior member support should be estimated when the Validation Plan is written, though flexibility must be allowed throughout the course of the evaluation. The support provided by the Chief Validator and senior members of the Validation Body should be as expeditious as possible. The Validator should give the Chief Validator and senior member a recommended deadline for any support that is requested.

8.2 Interpretations

8.2.1 Interpretation Sources

Three primary sources for interpretations of CC, CEM or CCEVS requirements are available to the Validator. These are the international interpretations of the CC and CEM issued by the Common Criteria Interpretations Management Board (CCIMB), the NIAP interpretations of the CC and CEM issued through the CCEVS, and CCEVS policy statements.

- **International Interpretations**: CCIMB interpretations of the CC or CEM are the official interpretation of a CC or CEM used by all international users of the Common Criteria. CCIMB interpretations take precedence over all other CC and CEM requirements, essentially replacing the text of the current documents. The CCIMB list of CC and CEM international interpretations is available at the web site URL: http://www.commoncriteria.org/ri/FinalRI/Final_Interpretations.html.

- **NIAP Interpretations:** The CCEVS administers a public interpretation board for issuing NIAP interpretations of the CC and CEM. The board receives CC and CEM issues needing clarification or formal interpretation from the Validation Body, Validator, the Observation Decision Review Board (ODRB), or the general public. The interpretation board draft interpretations, and facilitates public discussion of draft interpretations to ensure that diverse views are considered. Once all views are

considered and incorporated as appropriate, the proposed interpretations are submitted to the Director, CCEVS for approval. Once approved, these interpretations are considered NIAP interpretations, replacing the corresponding text in the CC and CEM for all evaluations conducted under the CCEVS. These NIAP interpretations apply to all new evaluations conducted under the CCEVS until rescinded or replaced by the CCIMB interpretations. NIAP interpretations are submitted to the CCIMB for international coordination as appropriate. The details of the public interpretation board operating procedures will be documented in a separate document. The list of NIAP CC and CEM interpretations can be found at the web site URL: http://niap.nist.gov/cc-scheme/iwg-cc-public/index.html.

- **CCEVS Policy Statements:** CCEVS policy statements are formally documented statements of CCEVS policy. CCEVS policy statements may result from questions for clarification of CCEVS documented processes, policies and procedures, or undocumented practices. Formal questions not associated with a particular evaluation should be submitted in the form of a letter to the CCEVS Director. The CCEVS will answer these questions by return letter.

  For CCTL clarification questions associated with a particular evaluation the questions should be submitted in the form of an OR. Policy statements resulting from an OR will be issued in the form of a CCEVS observation decision (OD) for that evaluation. Note that, like all ODs, such a policy statement is applicable only to the specific evaluation being addressed.

  Other forms of documented policy statements are those issued by the CCEVS in the form of official CCEVS policy notices, or formally issued page changes to CCEVS publications.

8.2.2 Applying Interpretations

All final NIAP and international common criteria interpretations as of the date of acceptance of the evaluation by the Validation Body for validation processing are mandatory for that evaluation. Interpretations accepted/approved after the start of an evaluation can be applied at the discretion of the CCTL and Sponsor. CCEVS policy statements are effective on the date issued, unless a different effective date is noted in the CCEVS notice of interpretation. The Validator is responsible for ensuring that all applicable interpretations have been incorporated as part of an evaluation.

8.3 NVLAP or CCEVS Remedial Action

If the Validator sees a pattern of deficiencies from a CCTL, the Validation Body management should be notified. Management will in turn notify NVLAP. In coordination with the Validation Body, NVLAP can investigate the source of the deficiencies, and require the laboratory to submit a plan to correct the problem. If a

laboratory fails to effectively correct the problem, NVLAP may suspend accredited status of the laboratory and the Director of the Validation Body could suspend the CCTL's authorization to conduct evaluations under the CCEVS until the problem is corrected.

8.4 Resolution Process for Evaluation Issues

There are numerous points in an evaluation when technical or process questions are posed to the Validation Body. It is the Validator's responsibility to represent the Validation Body and respond in a timely manner to these requests. It is the Validation Body's responsibility to support the Validators in this activity. The Validation Body maintains a process to support the Validators in their timely responses to the CCTL requests for evaluation decisions.

Issues fall into two broad categories: (1) those within the purview of the Validator to decide and (2) those either beyond this purview or for which the CCTL desires a formal Validation Body decision.

Observation Reports (ORs) are the vehicle for a CCTL to obtain formal, Validation Body approval for a proposed solution to an evaluation technical or process issue. An OR documents the CCTL concern and provides the mechanism for the CCTL to obtain a timely decision from the Validation Body on potential areas of misunderstanding. The Validator is responsible for aiding the CCTL in preparing the OR and for delivering the OR to the Validation Body for consideration. The Validation Body will review the OR and issue a response (called the Observation Decision or OD) back to the to the evaluation team via the Validator. An OD is issued for each OR submitted, and applies only to the evaluation for which the OR was submitted.

8.4.1 Observation Reports

An Observation Report (OR) enables the CCTL to obtain approval of a proposed solution to, or Validation Body direction for, an observed Common Criteria or Common Evaluation Methodology technical evaluation issue or Validation Body process issue (i.e., CCTL question, concern or problem). See Annex D for OR-OD format and content. The CCTL documents the evaluation or process issue in the OR, provides background information and, where possible, offers a proposed solution. The CCEVS Validation Body uses the OR to review the issue and develop clarification/guidance to the CCTL. The Validation Body uses an Observation Decision (OD) to formally respond to an OR. An OD is issued for each OR. The Validation Body's OR resolution process will usually be accomplished within eight (8) working days of the Chief Validator's receipt of a complete and unambiguous OR.

The OR-OD format and process described herein specifically addresses CCTL observation issues submitted to the Validation Body; that is, decisions not made by the Validator. For decisions made by the Validator, any reasonable documentation means

may be used, provided that all Validator decisions are documented and visible to both the CCTL and the Validation Body.

The CCTL uses its own procedures for observation reporting (and response) for CCTL to sponsor communications. Any Validator to sponsor observation issues should be addressed through the CCTL.

8.4.1.1 Submission of Observation Reports

The CCTLs should submit an OR when the underlying PP, the CC, CEM, or CCEVS policy is incomplete, unclear, inconsistent, or erroneous and existing CCEVS guidance is inadequate and either the:

1. Validator is unable or unwilling to provide the decision or
2. The CCTL desires a decision from the Validation Body.

A CCTL must submit ORs to the Validator assigned to the evaluation for which the OR was generated. An Observation Report should contain, at a minimum the following:

1. date of submission,
2. current projected evaluation completion date,
3. identity of the CCTL submitting the OR,
4. CCTL point of contact for the issue including contact information (e-mail and phone),
5. CCTL specific tracking ID (optional),
6. identity of the primary Validator for the evaluation including contact information (e-mail and phone),
7. evaluation for which the OR is being submitted,
8. evaluation target (which PP ST/TOE),
9. issue for which a resolution is requested,
10. state whether it is a CCEVS process issue or a technical evaluation issue,
11. proposed resolution to the issue and impact (may include various resolutions and respective impacts),
12. background explanation of the issue and of the proposed resolution, and
13. identification of information sources (i.e., references) used in preparing the OR.

Any information in the OR that is not publicly releasable must be explicitly marked by the CCTL. Each paragraph in the OR that contains proprietary information must be preceded by the notation “(PROP)” or “(P)”.

8.4.1.2 Handling of Observation Reports

Upon receiving the OR, the Validator will:

1. Verify that the OR submitted meets the format requirements,
2. Add to the background section their comments/reaction to the opinions expressed by the CCTL including whether the Validator concurs with the OR and any known precedents, prior guidance, ODs or interpretations on the issue,
3. Submit the OR with Validator comments to the ccevs-or@nist.gov mail list within three (3) business days. The Records Manager will in turn acknowledge receipt, assign a tracking number (i.e., CCEVS-OR-xxxx), and notify the Validator of the expected response date. The Validator will notify the CCTL that the OR was received and forwarded.

The Validator must explicitly mark (as noted in the previous section) any proprietary information used in Validator additions to the OR that is not publicly releasable.

The Chief Validator will forward issues that are primarily Validation Body process related to the Director CCEVS, with a copy to the Deputy Director CCEVS, for resolution.

8.4.2 Observation Decisions

An Observation Decision (OD) is issued in response to an OR. The OD is the formal documented response from the Validation Body that provides clarification/guidance to the CCTL on a submitted OR. Once an OD is rendered the Validator is responsible for forwarding the completed OD to ccevs-records@nist.gov mail list and to the CCTL. OR/ODs will use the tracking number assigned by the records manager as the record ID, i.e., CCEVS-OR/OD-xxx.

8.4.2.1 Application of Observation Decisions

The OD serves to provide the CCTL with confidence that the currently understood resolution will be honored for the evaluation in question when the final validation of evaluation results is conducted. The OD is applicable only for the issue identified in the OR and only for that evaluation. To this end, the OD represents Validation Body direction and policy provided. The CCTL is expected to apply the OD if:

1. The associated OR fully disclosed all relevant information that was known or should have been know to the CCTL; and

2. The evaluation has not exceeded its scheduled completion date by more than six months from the expected completion date indicated in the OR.

ODs provide the best answer available at the time, giving timely, good-faith guidance to CCTLs on a given evaluation. An OD is for a specific evaluation and is issued in a short

time frame to accommodate the CCTL evaluation schedule. This short time frame for the OD may not provide adequate time to develop confidence that the decision is correct and widely applicable. Therefore, the OD is applicable only to an OR for one evaluation and does not apply to future evaluations, even if the same issue should arise. Thus, until longer-term CCEVS guidance becomes available, the CCTL is expected to resubmit an OR for each evaluation to which the issue applies.

8.4.3 Appeal and Resolution of Observation Decision

The OD is the formal, documented response from the Validation Body providing clarification/guidance to the CCTL on a submitted OR. If the CCTL and/or sponsor disagree with an OD and wishes to formally appeal it, the Validation Body will reconsider the OD. To formally appeal the issued OD and request reconsideration the CCTL and/or sponsor shall:

1. Identify the OD and associated OR being appealed;
2. Identify each item of the OD that the CCTL is appealing;
3. Explain and justify why they disagree with the OD item;
4. Identify specific supporting references (document identification, section & paragraph) for all justifications where applicable;
5. Propose acceptable resolutions, revisions or alternatives to the OD;
6. Attach the original OR and corresponding OD; and
7. Submit the appeal documentation package to the CCEVS Director and a copy to the Deputy Director.

Upon receipt of the request for OD reconsideration, the CCEVS Director will acknowledge receipt of the appeal/reconsideration request within 3 business days. The CCEVS Director then reviews the request, consults with the involved parties about any clarifications as necessary, consults with other Validation Body resources as needed, and prepares a resolution for the appealed OD. The resolution may be to uphold the original OD or issue a revised OD. The decision is incorporated into the OD if it represents a change to the previous decision, and the CCTL, Chief Validator, and the Validator are notified as to the decision reached.

The OD appeal and resolution process ends when the CCEVS Director issues the response to the appeal. The resulting OD is used by the CCTL for the evaluation in question. The Validation Body will attempt to issue the appeal response within 15 working days from receipt of the OD request for reconsideration.

8.5 **CCEVS Communication Mechanisms**

CCEVS Mail Lists: E-mail Lists on the CCEVS mail server are available for communicating with (and receiving announcements from) the CCEVS. The e-mail list names and purpose of each mail list (ML) are described below.

cc-cmt@nist.gov [For public to submit comments on proposed NIAP interpretations to the CC & CEM]
cc-in@nist.gov [Self-subscribing ML for receiving announcements of NIAP CC & CEM Interpretations]
ccevs-announcements@nist.gov [Self-subscribing ML for receiving CCEVS announcements]
ccevs-comments@nist.gov [For public to submit questions and comments to the CCEVS staff]
ccevs-evalsubmits@nist.gov [Internal ML used by CCTL's for submitting new Evaluation Acceptance Packages to the CCEVS]
ccevs-labapplicants@nist.gov [Self-subscribing ML for receiving information of interest to applicants who are considering becoming a Common Criteria Testing Laboratory]
ccevs-labs@nist.gov [ML of CCTL directors primarily used by the CCEVS staff for sending information to CCEVS-Approved CCTLs]
ccevs-or@nist.gov [internal CCEVS ML used by Validators for submitting Observation Reports to CCEVS]
ccevs-records@nist.gov [Internal CCEVS ML used by CCEVS staff and Validators for submitting records of validation activities]
ccevs-staff@nist.gov [Internal CCEVS ML for sending messages to CCEVS management and operation staff]
ccevs-validators@nist.gov [Internal ML of CCEVS Validators]

ValGrams: ValGrams are e-mail messages sent to Validators by the Chief Validator or CCEVS staff with important information or reminders concerning validation processes, policies or procedures. ValGrams are the primary mechanism the Validation Body uses for directly communicating with all Validators. ValGrams are typically distributed via the **ccevs-validators@nist.gov** mail list, and often contain instructions that Validators must apply immediately in validations.

CCEVS Newsletters: The CCEVS periodically issues newsletters containing information of general interest to the CCEVS community. CCEVS newsletters are another resource for Validators to use to keep up-to-date on CCEVS news. CCEVS newsletters are typically distributed via the ccevs-announcements@nist.gov mail list. Subscribers on the ccevs-validators@nist.gov mail list are automatic subscribers of the ccevs-announcements@nist.gov mail list.

(This page intentionally left blank)

Annex A. Acronym List

CC	Common Criteria
CEM	Common Evaluation Methodology
CCRA	Common Criteria Recognition Arrangement
CCTL	Common Criteria Testing Laboratory
CCEVS	Common Criteria Evaluation and Validation Scheme
ETR	Evaluation Technical Report
EAP	Evaluation Acceptance Package
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
NIAP	National Information Assurance Partnership
MR	Memorandum for Record
MSR	Monthly Summary Report
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
OD	Observation Decision
OR	Observation Report
ODRB	Observation Decision Review Board
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
URL	Uniform Resource Locator
VID	Validation Identification Number

VP	Validation Plan
VPL	Validated Products List
VR	Validation Report

Annex B. Glossary of Terms

This glossary contains definitions of terms used in the Common Criteria Scheme. These definitions are consistent with the definitions of terms in ISO Guide 2 and also broadly consistent with the Common Criteria and Common Methodology. However, the definitions of terms may have been amplified to add greater clarity or to interpret in the context of the evaluations conducted within the scheme.

Accredited: Formally confirmed by an accreditation body as meeting a predetermined standard of impartiality and general technical, methodological, and procedural competence.

Accreditation Body: An independent organization responsible for assessing the performance of other organizations against a recognized standard, and for formally confirming the status of those that meet the standard.

Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security (CCRA): An arrangement whereby the Parties (i.e., signatories from participating nations) commit themselves (with respect to IT products and protection profiles) to recognize the Common Criteria certificates issued by any one of them under the terms of the Agreement.

Appeal: The process of taking a complaint to a higher level for resolution.

Approval Policy: A part of the essential documentation of the Common Criteria Evaluation and Validation Scheme. The policy documents:

1. The procedures for application to become a CCTL;
2. The procedures for a CCTL to be placed on the NIAP Approved Laboratories List;
3. A description of the methods used by NIAP for processing CCTL applications; and
4. The requirements to be met by a CCTL applicant in order to qualify.

Approved CCTL: Assessed by the CCEVS Validation Body as technically competent in the specific field of IT security evaluation and formally authorized to carry out evaluations within the context of the Common Criteria Evaluation and Validation Scheme.

Approved Laboratories List: The list of approved CCTLs authorized by the CCEVS Validation Body to conduct IT security evaluations within the NIAP CCEVS.

Approved Test Methods List: The list of approved test methods maintained by the CCEVS Validation Body that can be selected by a CCTL in choosing its scope of accreditation, that is, the types of IT security evaluations that the CCTL will be authorized to conduct using NIAP-approved test methods.

Availability: The prevention of unauthorized withholding of information resources.

CCEVS Validation Body: a government organization responsible for carrying out validation and for overseeing the day-to-day operation of the CCEVS.

Chief Validator: The Validation Body staff member responsible for providing direction to Validators on technical issues, and for reviewing and approving technical work produced by Validators.

Common Criteria (CC): Common Criteria for Information Technology Security Evaluation, the title of a set of documents describing a particular set of IT security evaluation criteria.

Common Evaluation Methodology (CEM): Common Methodology for Information Technology Security Evaluation: a technical document that describes a set of IT security evaluation methods.

Common Criteria Certificate: A brief public document issued by the CCEVS Validation Body under the authority of NIST and NSA which confirms that an IT product or protection profile has successfully completed evaluation by a CCTL. A Common Criteria certificate always has an associated validation report.

Common Criteria Evaluation and Validation Scheme (CCEVS): The program developed by NIST and NSA as part of the National Information Assurance Partnership (NIAP), establishing an organizational and technical framework to evaluate the trustworthiness of IT products and protection profiles under the Common Criteria for IT Security Evaluation.

Common Criteria Testing Laboratory (CCTL): an IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations under.

Complaint: A written formal allegation or disagreement against a party.

Complainant: The party initiating a complaint.

Confidentiality: The prevention of unauthorized disclosure of information.

Deliverables List: A document produced by a CCTL containing the list of documents comprising the security target, all representations of the TOE, and developer support required to conduct an IT security evaluation in accordance with the CCTL's Evaluation Work Plan.

Evaluation: The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated. CEM.

Evaluation Evidence: Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.

Evaluation and Validation Scheme: The systematic organization of the functions of evaluation and validation within a given country under the authority of a Validation Body in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved.

Evaluation Schedule: The schedule established by a CCTL for the conduct of an IT security evaluation.

Evaluation Technical Report (ETR): A report giving the details of the findings of an evaluation, submitted by the CCTL to the CCEVS Validation Body as the principal basis for the validation report.

Evaluation Work Plan: a document produced by a CCTL detailing the organization, schedule, and planned activities for an IT security evaluation.

Integrity: The prevention of the unauthorized modification of information.

Interpretation: expert technical judgment, when required, regarding the meaning or method of application of any technical aspect of the Common Criteria and/or Common Evaluation Methodology.

IT Product: a package of IT hardware, software, and/or firmware providing functionality designed for use or incorporation within a multiplicity of IT systems.

IT System: a group of IT products, either tightly or loosely coupled, working together in a specific configuration to provide a capability or system solution to a consumer in response to a stated need.

IT Security Evaluation Criteria: a compilation of the necessary information to be provided and the actions to be taken in order to provide grounds for confidence that security evaluations will be carried out effectively and to a consistent standard.

IT Security Evaluation Methodology: a methodology to be used by evaluation facilities in applying IT security evaluation criteria in order to give grounds for confidence that evaluations will be carried out effectively and to a consistent standard.

National Voluntary Laboratory Accreditation Program (NVLAP): the U.S. accreditation authority for CCTLs operating within the NIAP Common Criteria Evaluation and Validation Scheme.

Observation Reports (OR): a report issued to the CCEVS Validation Body by a CCTL or sponsor identifying specific problems or issues related to the conduct of an IT security evaluation.

Protection Profile (PP): an implementation independent set of security requirements for a category of IT products that meet specific consumer needs.

Records Manager: The Validation Body staff member responsible for coordinating and maintaining the Validation Body Record System.

Recognition of Common Criteria Certificates: With respect to the *Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security*, acknowledgement by one party of the validity of the Common Criteria certificates issued by another Party.

Scope of Accreditation: the NIAP-approved test methods for which a CCTL has been accredited by NVLAP.

Security Target (ST): a specification of the security required (both functionality and assurance) in a Target of Evaluation (TOE), used as a baseline for evaluation under the Common Criteria. The security target specifies the security objectives, the threats to those objectives, and any specific security mechanisms that will be employed.

Sponsor: the person or organization that requests a security evaluation of an IT product or protection profile.

Target of Evaluation (TOE): a group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC. Also, a protection profile that is the subject of a security evaluation under the Common Criteria.

Test Method: an evaluation assurance package from the Common Criteria, the associated evaluation methodology for that assurance package from the Common Evaluation Methodology, and any technology-specific derived testing requirements.

Validation: The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.

Validation Body: A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

Validated Products List (VPL): a publicly available document issued periodically by the CCEVS Validation Body giving brief particulars of every IT product/system or protection profile that holds a valid Common Criteria certificate awarded by the CCEVS Validation Body and every product or profile validated or certified under the authority of authority of another CCRA party for which the certificate has been recognized.

Validation Report (VR): a publicly available document issued by the CCEVS Validation Body that summarizes the results of an evaluation and confirms the overall results (i.e., that the evaluation has been properly carried out, that the Common Criteria, the Common Evaluation Methodology, and the scheme-specific procedures have been correctly applied; and that the conclusions of the ETR are consistent with the evidence adduced).

(This page intentionally left blank)

Annex C. Validation Guidance for CEM Work Units

The guidance provided in this Annex is based on suggestions from current understanding of the CC, CEM and associated interpretations thereof. In applying these guidelines the Validator should carefully consider applicability of this guidance to the actions and situations as they apply to the specific evaluation being conducted. Further, current NIAP and CCIMB interpretations of CC and CEM should always take precedence over any guidance offered herein.

In each section below validation guidance is given to the Validator. One form of Validator guidance describes what the Validator should be expecting to see in the CCTL's reporting of evaluation activities and results thereof. The other form of Validator guidance is simply additional information for Validators about the CC and the CEM so that the Validator is better able to understand how the evaluation should be done, and thus is better able to make an assessment of the evaluation effort.

The guidance is categorized according to the general area in which evaluation analysis is performed (e.g., "Configuration Management", "Developmental Documentation", etc.). If the Validator expects the CCTL to review evaluation evidence to aid in the evaluation analysis, the appropriate CC element is referenced so the Validator knows which evidence should be looked at. If the Validator expects the CCTL to witness an evaluation activity, or if the CEM clarifies what the evaluation is expected to do or provide, a reference to the appropriate CEM work unit is provided. The Validator is expected to keep records of interactions with the evaluators, to document what and how verification of evaluation activities/results were done, the guidance provided, deficiencies identified, and evaluation corrections made.

C.1 Delivery and Operation (ADO)

C.1.1 Installation of the TOE Validation

Work Units: EAL1:ADO_IGS.1-2, 1:ATE_IND.1-2
Work Units: EAL2:ADO_IGS.1-2, 2:ATE_IND.2-2
Work Units: EAL3:ADO_IGS.1-2, ATE_IND.2-1, ATE_IND.2-2, AVA_MSU.1-6, AVA_MSU.1-7
Work Units: EAL4:ADO_IGS.1-2, ATE_IND.2-1, ATE_IND.2-2, AVA_MSU.2-7, AVA_MSU.2-8

Validator Guidance: The Validator needs to determine that the CEM work units were performed in the proper order (i.e., ADO_IGS work units are performed before ATE_IND work units) and that nothing was "missed" with respect to the installation and configuration of the TOE. The ETR, evaluation records, and interaction with the evaluators should show that vendor provided installation, generation, and start-up evidence (ADO_ISG.1.1C) for the product were examined. Additionally, an explanation (possibly including examples from vendor provided evidence) should be provided as to how work unit order occurred and how it was concluded that nothing was missing in the

installation and configuration of the TOE.

The Validator needs to determine that all parts of the system are "covered". For example, if the TOE consists of a firewall on top of a commercial operating system, then the evaluation information should show that both the firewall and commercial operating system installation and configuration documents are examined. Note that if the TOE is only a portion of the system (that is, there are requirements on the IT Environment), then only the TOE guidance has to be examined.

The Validator needs to determine that independent testing was performed on the platform included in the evaluated configuration and not some special platform that is useful only for testing. In this vein, the ETR and/or evaluation records should define whether or not any test artifacts (e.g., special test "middleware" or a test harness) were used by either the vendor or the CCTL. If this is the case then the documented analysis must show that these test artifacts (e.g., middleware or harness) does not affect the validity of the testing effort with respect to the security properties of the system.

C.1.2 Delivery Procedure Validation

Work Units: EAL3: ADO_DEL.1-3
Work Units: EAL4: ADO_DEL.2-5

Validator Guidance: It will do no good to the end users if the mechanisms of the system can be circumvented by modifying the TOE so that mechanisms are ineffective, or if they can be spoofed into loading a patch that will circumvent the security mechanisms. The Validator should review the evaluation findings for work units. If the analysis does not appear adequate the Validator should discuss their review with the CCTL. This is largely a subjective work item so the Validator should take into account the intended environment for the TOE under evaluation. For instance, if the environment is one in which the TOE will be purchased "off the shelf", commercial shrink-wrapped distribution of the software portion of the TOE may be adequate, because it would most likely be impractical for the "bad guys" to modify every copy in transit in hopes that they would modify the one copy that was going to be used in the target environment.

Work Units : EAL4: ADO_DEL.2-3:

Validator Guidance: The Validator needs to determine if the CCTL records recognize the distinction between ADO_DEL.2-3 work unit and ADO_DEL.2-1 work unit. The work unit ADO_DEL.2-1 deals with the integrity of the TOE when it is delivered from the vendor to the user. However, this work unit ADO_DEL.2-3 deals with means by which a consumer is able to verify that the TOE, including a supplemental patches or updates, actually came from the vendor and not someone with a CD-writer and a color printer.

C.2 Guidance Documentation (AGD)

C.2.1 Administrative Guidance Validation

Work Units EAL1: AGD_ADM.1-1, AGD_ADM.1-2, AGD_ADM.1-3, AGD_ADM.1-5
Work Units EAL2: AGD_ADM.1-1, AGD_ADM.1-2, AGD_ADM.1-3, AGD_ADM.1-5
Work Units EAL3: AGD_ADM.1-1, AGD_ADM.1-2, AGD_ADM.1-3, hAGD_ADM.1-5
Work Units EAL4: AGD_ADM.1-1, AGD_ADM.1-2, AGD_ADM.1-3, AGD_ADM.1-5

Validator Guidance: A large percentage of security breaches occur because systems that are supposed to be providing the security are incorrectly administered. The Validator should keep in mind that it is more important that "big picture" issues are addressed in the analysis and that the CCTL is educated (if necessary) on performing CC evaluations rather than ensuring every last detail is correct, spelling is checked, etc. The ability of the CCTL to identify problems in the guidance (e.g., a subsystem or class of interfaces missing from the documentation, lack of guidance on security-critical commands or GUI options) should be the focus of this validation action.

The Validator needs to determine that the CCTL has a methodology for identifying the security functions and interfaces that the administrator must address. The CCTL should have a methodology for performing this identification task (e.g., examining the TSS in the ST for security functions, looking at the FMT components for administrative-guidance-related management tasks, checking the FS for interfaces). The Validator also needs to understand how the CCTL performs the work units for AGD_ADM.1-7C. For this work unit the evaluator determines whether the administrative guidance is "consistent with all other documentation supplied for evaluation." While the AGD requirements stay the same for all EALs, the number and complexity of the "other documentation supplied for evaluation" increases as the EAL increases. The Validator, therefore, needs to determine if the CCTL recognizes this fact and accounts for it in its work plan for the affected work units.

Furthermore, for AGD-required consistency analyses, the CCTL needs to recognize the need to record results for each consistency analysis that it performs (e.g., administrative guidance with functional specifications, administrative guidance with vulnerability analysis, administrative guidance with installation, generation, and start-up procedures --- that's 3 analyses for this example).

C.2.2 User Guidance Validation

Work Units EAL1: AGD_USR.1-1, AGD_USR.1-2, AGD_USR.1-3
Work Units EAL2: AGD_USR.1-1, AGD_USR.1-2, AGD_USR.1-3
Work Units EAL3: AGD_USR.1-1, AGD_USR.1-2, AGD_USR.1-3
Work Units EAL4: AGD_USR.1-1, AGD_USR.1-2, AGD_USR.1-3

Validator Guidance: The Validator should keep in mind that it is more important that "big picture" issues are addressed in the evaluation analysis and that the TOE user guidance has addressed each major security mechanism (logging in, discretionary access controls, etc.) with which the untrusted user is expected to interact. The review of the evaluation analysis should allow the Validator to determine that any serious deficiencies found when the CCTL performed its review have been noted and corrected.

The Validator needs to determine that the CCTL has a methodology for identifying the security functions and interfaces that the user must address. The CCTL should have a methodology for performing this identification task (e.g., examining the TSS in the ST for security functions, looking at the FMT components for administrative-guidance-related management tasks, checking the FS for interfaces). The Validator also needs to determine how the CCTL performs the work units for AGD_USR.1-5C. For this work unit the evaluator determines whether the user guidance is "consistent with all other documentation supplied for evaluation." While the AGD requirements stay the same for all EALs, the number and complexity of the "other documentation supplied for evaluation" increases as the EAL increases. The Validator, therefore, needs to determine if the CCTL recognizes this fact and accounts for it in its work plan for the affected work units.

Furthermore, for AGD-required consistency analyses, the CCTL needs to recognize the need to record results for each consistency analysis that it performs (e.g., user guidance with functional specifications, user guidance with vulnerability analysis, user guidance with installation, generation, and start-up procedures --- that's 3 analyses for this example).

C.3 Development (ADV)

C.3.1 Functional Specification Validation

Work Units EAL2: ADV_FSP.1-3, ADV_FSP.1-5

Validator Guidance: The goal for the Validator in this work unit is to determine whether the CCTL is performing the correct analysis given the evidence. The Validator should review the evaluation records to determine that no significant area of the documentation has been overlooked by the CCTL with respect to the functional specification (for instance, if doing a firewall evaluation ensure that the operating system interfaces presented to administrators are not overlooked as part of the TSFI. In performing their review, Validators should determine that all documents referenced by the functional specification (if any) are available to the CCTL. The evaluation analysis needs to show that the referenced material contains the appropriate information (some functional specifications are merely "pointer" documents, so the documents referenced by these pointers must also be examined). With respect to each interface, the Validator needs to determine that the CCTL has considered error messages, exceptions, and effects of an interface in their analysis. For instance, it is common in some documentation to simply group all possible error messages in one chapter, and not tie these error messages to a single interface. This does not meet the requirement; the error messages needs to be associated with each interface.

Work Units EAL2: ADV_FSP.1-2
EAL3: ADV_FSP.1-2; ADV_HLD.2-2
EAL3: ADV_FSP.2-2, 1-8; ADV_HLD.2-2; ADV_LLD.1-2

Validator Guidance: CCTLs sometimes have difficulty determining what they should do with respect to internal consistency. There are two major issues with this work unit: one concerning how the CCTL goes about performing the action, and one concerning how the CCTL reports this action in the ETR.

CCTLs should have a methodology for performing an internal consistency check; this will aid not only in consistent results, but also in reporting those results. This methodology should include some notion of checking multiple sources of information if present; this is especially relevant if the functional specification is contained in more than one document. The methodology should also include some notion of checking for interfaces with similar functionality, as well as the obvious check for interfaces described in multiple places (within the same document or in different documents). It should be noted that this work unit is not the place where checks against other documentation, such as the high-level design, are made.

The Validator should not accept a rationale in the ETR for this work unit that merely states "The functional specification was examined and no inconsistencies were found." As a minimum, the ETR should report how the examination was carried out, and what specific documentation was examined. The Validator should also expect some summary

(preferably in the ETR, but possibly via CCTL records) of the problems found in various versions of the FSP related to this work unit, giving the Validator confidence that the work was actually performed by the CCTL.

Work Units EAL2: ADV_FSP.1-4
EAL3: ADV_FSP.1-4
EAL4: ADV_FSP.2-4

Validator Guidance: The point of these work units (as noted in the informative text in the CEM for this work unit) is one of definition of the TSF. The CCTL must have a sense of everything that the TOE includes, and what is part of the TSFI (security-relevant) and what is not in order to determine that all of the external TSFI have been described. The Validator needs to determine that the CCTL understands that they must have sufficient information about the interfaces that are not considered part of the TSFI, and to determine that they have been correctly classified by the provider of the functional specification. For those interfaces that *are* part of the TSFI, the CCTL needs a further description of their characteristics in accordance with work unit ADV_FSP.1-5. , or ADV_FSP.2-5. If necessary, the Validator should determine that the CCTL understands the identification of the TSFI from all of the interfaces presented by the TOE is something that needs to be done by the CCTL and done early in the evaluation, so that "surprises" (e.g., finding a security-relevant subsystem late in the evaluation) are minimized.

At EAL4, these work units require an argument that the decomposition presented in the evidence (that is, the TSFI for the functional specification; the subsystems for the high-level design; and the modules for the low-level design) completely and accurately represent the *functional requirements* in the ST, *not* the security functions. It is also not an internal consistency analysis, as appears to be described in the informative text associated with ADV_LLD.1-11.

It is also recommended that the correspondence be made directly, and not via arguments about the RCR analysis, security functions, etc. Those arguments are presented elsewhere, and the evaluator merely pointing to this evidence adds no value to the analysis. Finally, it should be noted that a mapping alone is not sufficient justification in the ETR; prose is needed to explain how the mapping was developed, and how that process (coupled with the mapping) helps ensure that the representations are complete and accurate with respect to the SFR.

Work Units EAL2: ADV_FSP.1-7, 1-8
EAL3: ADV_FSP.1-7, 1-8; ADV_HLD.2-11,2-12

Validator Guidance: The Validator needs to determine that the CCTL understands the following about these work units. First, these work units are to be performed by the evaluation CCTL, and not by the vendor. As such, the Validator should see evidence of this work at least in the ETR, and may wish to examine the records kept of this activity by the CCTL in order to gain more insight into what was actually done. Secondly these work units require an argument that the TSFI presented in the functional specification completely and accurately represents the *functional requirements* in the ST, *not* the

security functions. It is also recommended that the correspondence be made directly, and not via arguments about the RCR analysis, security functions, etc. Finally, it should be noted that a mapping alone is not sufficient justification in the ETR; prose is needed to explain how the mapping was developed, and how that process (coupled with the mapping) helps ensure that the TSFI are complete and accurate with respect to the SFR.

C.3.2 High-Level Design Validation

Work Units EAL2: ADV_HLD.1-4

Validator Guidance: In determining whether the CCTL is performing the correct analysis of the evidence, the Validator needs to determine that CCTL has correctly addressed the following two issues in their analysis. First, the TSFI should be fully represented by the subsystem description. Second, each subsystem should have an adequate description of its security functionality.

The first item is basically a "big picture" check, where based on the CCTL's understanding of what makes up the TSF (as opposed to the larger TOE). In the case of a TOE consisting of a firewall and operating system with hardware in the IT environment, this would involve ensuring that the high-level design included descriptions (in terms of subsystems) of the firewall component, and the operating system component. The Validator should check the CCTL's analysis to ensure that 1) they have performed this analysis in more detail for the entire set of subsystems and 2) they have correctly identified any deficiencies in this area.

The second item is to ensure that "right stuff" is being described in the various subsystem descriptions. The Validator should determine that the CCTL looked to see that at a minimum: the security-relevant functions are being described and described in enough detail to provide useful information about the design of the security- relevant parts of the system (if it is not, then the evaluation CCTL cannot do their analysis adequately).

Work Units EAL2: ADV_HLD.1-2

Validator Guidance: CCTLs sometimes have difficulty determining what they should do with respect to internal consistency. There are two major issues with this work unit; one concerning how the CCTL goes about performing the action, and one concerning how the CCTL reports this action in the ETR.

CCTLs should have a methodology for performing an internal consistency check; this will aid not only in consistent results, but also in reporting those results. In addition to checking places where a subsystem (or a portion of a subsystem) is described more than once, this methodology should include some notion of checking multiple sources of information if present; this is especially relevant if the high-level design is contained in more than one document. It should be noted that this work unit is not the place where checks against other documentation (e.g., the functional specification) are made.

In documenting the results, the Validator should not accept a rationale in the ETR for this work unit that merely states "The high-level design was examined and no inconsistencies

were found." As a minimum, the ETR should report how the examination was carried out, and what specific documentation was examined. The Validator should also expect some summary (preferably in the ETR, but possibly via conversations with CCTL personnel) of the problems found in various versions of the high-level design related to this work unit, giving the Validator confidence that the work was actually performed by the CCTL.

Work Units EAL2: ADV_HLD.1-5, 1-6

Validator Guidance: These work units are applicable only if the TOE is not a complete system; that is, if there are requirements on the IT Environment. If there are requirements on the IT environment, then the level of detail required in the high-level design with respect to these work units should be defined in terms of what information is need to successfully "compose" two (or more) evaluated products to make a trusted system.

Work Units EAL2: ADV_HLD.1-9, 1-10

Validator Guidance: The Validator should determine that the CCTL understands the following about these work units. First, these work units are to be performed by the evaluation CCTL, and not by the vendor. As such, the Validator should see evidence of this work at least in the ETR, and may wish to examine the records kept of this activity by the CCTL in order to gain more insight into the specific worked performed. Secondly, these work units require an argument that the functionality (and interfaces) described in the high-level design completely and accurately represent the *functional requirements* in the ST, *not* the security functions. It is also recommended that the correspondence be made directly, and not via arguments about the RCR analysis, security functions, etc. Finally, it should be noted that a mapping alone is not sufficient justification in the ETR; prose is needed to explain how the mapping was developed, and how that process (coupled with the mapping) helps ensure that the subsystem descriptions are complete and accurate with respect to the SFR.

Work Units EAL4: ADV_HLD.2-10; ADV_LLD.1-10

Validator Guidance: The Validator should note that these work units do not *mandate* that the system be separated into TSP-enforcing and "other" subsystems/modules; it only states that this separation must be described (if present). The informative text does not clearly indicate a difference between TSP-enforcing and TSP-supporting in terms of this requirement. Instead, it states the somewhat obvious fact that all TSP-enforcing subsystems are part of the TSF, without addressing (directly) TSP-supporting subsystems. This can potentially be very confusing to evaluators, and the Validator should clarify that this requirement is not requiring separation of any kind, and the description that needs to be present should probably be no more than a description of what subsystems/modules are part of the TSF and what are not. If the vendor wants to tackle the larger problem of TSP-enforcing vs. TSP-supporting, that is allowed but not required. If the vendor does make the argument, the Validator needs to determine that the CCTL evaluates that argument.

C.3.3 Correspondence Analysis Validation

Work Units EAL2: ADV_RCR.1-1, 1-2

Validator Guidance: The correspondence evidence called for by ADV_RCR.1.1C is required to be delivered as evidence by the vendor, meaning that the evaluator's role is to confirm the developer's analysis. The evaluator can attempt to analyze the vendor-provided guidance directly, or the evaluator can perform the correspondence activity himself or herself and then compare their results with the vendors. In either case, the analysis provided by the vendor must be more than just a mapping; prose must accompany any mapping describing how correctness and completeness are verified. Similarly, the evaluator's rationale in the ETR must discuss how they determined that the vendor's analysis was adequate, and not merely be a statement of adequacy.

C.3.4 TSF Identification Validation

Work Units EAL3: ADV_FSP.1-3, ADV_HLD.2-8

Validation Actions: The Validator needs to determine that the CCTL has correctly identified the TSF portion of the TOE. The Validator should review the CCTL evaluation analysis of this area, and determine that the TSF portion of the TOE was correctly identified., i.e., the CCTL examined the functional specification and high-level design evidence at a high level and, using their knowledge of the system, assess whether the interfaces identified seems complete with respect to the underlying system.

It is important to note that this activity does not call for a cross-reference matrix or a similar document, but is instead a "big-picture" judgment by the Validator based on the TOE and the evaluator's analysis. The Validator should keep in mind that the TOE is defined by the CC to consist of the product (hardware and software), the administrative guidance and the user guidance, and based on NIAP interpretation I-0411 also includes the ADO and ALC_FLR flaw remediation documents. The software part of the TOE consists of the TSF, which are the security-relevant pieces of the system (including otherwise untrusted tools used by the administrator to perform their administrative tasks), and "everything else" (e.g., application programs, games, word processors). Further, the software portion of the TOE is that software which is resident and accessible on a system after all of the vendor-provided installation procedures have been completed. For instance, if a CD contains the universe of (optional) programs that could be installed along with an operating system, and the IGS guidance only said to install three programs, then only those three programs (and not everything on the CD) would be included as the software part of the TOE.

In reviewing the CCTL's analysis, the Validator should look for some indication of the methodology used by the CCTL, which will allow the Validator to assess whether the described methodology is likely to produce the desired result if followed by the CCTL. For all software that is part of the TOE, the CCTL records should be able to demonstrate to the Validator how they assessed the ways in which an external entity (administrative or

otherwise) can interact with the software. These can be fairly straightforward, such as via an application programming interface or an administrative Graphical User Interface (GUI), but they can also be non-obvious, such as a protocol stack (at all layers, not just the application layer) or a configuration file read by a program on start-up. External interfaces described at the lower level of decomposition represented by the HLD should appear in the functional specification.

Work Units EAL4: ADV_FSP.2-3, ADV_FSP.2-7, ADV_HLD.2-8, ADV_LLD.1-8

Validation Actions: The Validator needs to determine that the CCTL has correctly identified the TSF portion of the TOE. To do this, the CCTL must have examined the functional specification, high-level design, and low-level design evidence and, using their knowledge of the system, assessed whether the interfaces identified seem complete with respect to the underlying system. The Validator should then review the records of CCTL analysis of this area to determine that the analysis has been done and all issues have been identified. This activity does not call for a cross-reference matrix or a similar document, but is instead a "big-picture" judgment by the Validator based on the TOE and the evaluator's analysis.

The Validator should keep in mind that the TOE is defined by the CC to consist of the product (hardware and software), the administrative guidance, and the user guidance. The software part of the TOE consists of the TSF, which are the security-relevant pieces of the system (including otherwise untrusted tools used by the administrator to perform their administrative tasks), and "everything else" (e.g., application programs, games, word processors). Further, the software portion of the TOE is that software that is resident and accessible on a system after all of the vendor-provided installation procedures have been completed. For instance, if a CD contains the universe of (optional) programs that could be installed along with an operating system, and the IGS guidance only said to install three programs, then only those three programs (and not everything on the CD) would be included as the software part of the TOE. The Validator should communicate this to the CCTL if the CCTL appears confused in this area.

In order to properly review the CCTL's analysis in this area, the Validator needs to be familiar with the software that is installed when the TOE is installed, and whether that software should be part of the TOE or not. For all software that is part of the TOE, the Validator should assess from the CCTL analysis the ways in which an external entity (administrative or otherwise) can interact with the software. These can be fairly straightforward, such as via an application programming interface or an administrative Graphical User Interface (GUI), but they can also be non-obvious, such as a protocol stack (at all layers, not just the application layer) or a configuration file read by a program on start-up. External interfaces described at the lower levels of decomposition (HLD and LLD) should appear in the functional specification. In reviewing the CCTL's analysis, the Validator should look for some indication of the methodology used by the CCTL, which will allow the Validator to assess whether the described methodology is likely to produce the desired result if followed by the CCTL.

C.3.5 Developmental Activities Validation

Work Units EAL3: ADV_HLD.2-5, 2-6
EAL4: ADV_HLD.2-5, 2-6

Validator Guidance: These work units are applicable only if the TOE is not a complete system; that is, if there are requirements on the IT Environment. If there are requirements on the IT environment, then the level of detail required in the high- level design with respect to these work units should be defined in terms of what information is needed to successfully "compose" two (or more) evaluated products to make a trusted system.

Work Units EAL3: ADV_HLD.2-10

Validator Guidance: The Validator should note that these work units do not *mandate* that the system be separated into TSP-enforcing and "other" subsystems; it only states that this separation must be described (if present). The informative text for this work unit in the CEM does not clearly indicate a difference between TSP-enforcing and TSP-supporting in terms of this requirement. Instead, it states the somewhat obvious fact that all TSP-enforcing subsystems are part of the TSF, without addressing (directly) TSP-supporting subsystems. This can potentially be very confusing to evaluators, and the Validator should clarify that this requirement is not requiring separation of any kind, and the description that needs to be present should probably be no more than a description of what subsystems are part of the TSF and what are not. If the vendor wants to tackle the larger problem of TSP-enforcing vs. TSP-supporting, then that is allowed but not required. If the vendor does make the argument, the Validator should ensure that the CCTL evaluates that argument.

C.3.6 Implementation Subset Validation

Work Units EAL4: ADV_IMP.1-2

Validator Guidance: At EAL4, the developer only needs to provide a subset of the implementation to meet the ADV_IMP.1-2 work unit. The CEM provides general guidance; the Validator needs to determine that the CCTL sample "makes sense" with respect to the system under examination, and is consistent with other evaluation efforts for products of similar size and scope. Finally, the Validator needs to review the CCTL's analysis with respect to the adequacy of the sample provided by the vendor, and provide the CCTL feedback on any deficiencies that are found. The Validator should discuss consistency issues with the CCTL, as appropriate.

(This page intentionally left blank)

C.4 Tests (ATE)

C.4.1 Functional Testing Validation

Work Units EAL2: ATE_FUN.1-4
EAL3: ATE_FUN.1-4
EAL4: ATE_FUN.1-4

Validator Guidance: The primary goal of the Validator with respect to functional testing is determination of the CCTL's understanding of the testing needed, and applies mainly to the case where the vendor is proposing a wide variety of platforms to be included in the TOE. This applies not only to various types of hardware, but also to various operating systems if a firewall or database or other application is the main focus of the vendor. In order to accomplish these aims, the Validator needs to first determine that the test plan (ATE_FUN.1.2C) was reviewed for the following information.

The test plan should describe the tested configurations in enough detail so that there is no ambiguity about what exactly comprises the TOE to be tested. For instance, if the hardware of the TOE includes 3 different, specific, Ethernet controllers, the test documentation should specify which ones would be used. Following this review, the Validator should check the CCTL's analysis of the plan in this area, as well as the argument for why the configuration chosen is sufficiently representative of the system that will eventually be given the rating.

C.4.2 Test Coverage Validation

Work Units EAL3: ATE_COV.2-4
EAL4: ATE_COV.2-4

Validator Guidance: The Validator needs to determine that the CCTL has performed a correct and complete coverage analysis with respect to the coverage of the TSFI by the tests as described in the test documentation (ATE_COV.2.2C). The Validator needs to determine from the CCTL analysis that all of the major groupings of interfaces have tests, and that the test appear to be of a similar level of detail. One area that is often missed is testing of the administrative interface and protocol interfaces, so the Validator should pay particular attention to determining that those interfaces are identified in the vendors test coverage analysis. The Validator should review the CCTL's analysis or discuss this analysis with the CCTL members responsible for performing it to determine that they have correctly identified any discrepancies that the vendor may have had. This process also enables the Validator to gain reasonable confidence that the CCTL's methodology for doing the analysis is sound.

C.4.3 Independent Testing Validation

Work Units EAL2: ATE_IND.2-7
EAL3: ATE_IND.2-7, ATE_IND.2-9, ATE_IND.2-10
EAL4: ATE_IND.2-7, ATE_IND.2-9, ATE_IND.2-10

Validator Guidance: Work unit ATE_IND.2-7 calls for the creation of a report on the independent testing effort by the CCTL personnel. The Validator should review the evaluation analysis with the goal of determining that it satisfies the requirements of the work unit. Because testing does not have to be complete at EAL2, the purpose of the review is not so much to determine if the evaluation CCTL "missed" anything, but rather to review the information produced by the CCTL to determine that it satisfies the requirement. If the body of evaluation analysis and evidence is large, the Validator may wish to sample the information recorded by the evaluators. For every test in the test subset that the Validator examines, the Validator should determine that all of the information mentioned in the work unit is recorded correctly, and that it is accurate. This includes determining that the test actually tests the security-relevant behavior that is presented at the interface being tested; that all necessary instructions (setup, tear-down, etc.) are present; and that there is evidence that the CCTL actually performed the test. In areas that the Validator notes deficiencies, efforts should be made to determine that the CCTL understands the issues that the Validator sees. The Validator should also discuss with the CCTL how they went about formulating their test subset, and how it augments the developer's testing effort. The Validator should write a summary of their findings in the validation report.

In addition to the analysis of the CCTL-produced report, the Validator should also interact with the CCTL as they perform work units ATE_IND.2-9 and ATE_IND.2-10.

The Validator is not to perform the testing or choose the sample as described in these work units. First, the Validator should assess the sample chosen by the CCTL, and make a determination whether that sample is sufficiently representative. It is expected that the Validator will interact with the CCTL in discussing this issue.

Second, the Validator should attend the testing performed by the CCTL. During this time the Validator should determine that the CCTL is running the subset chosen, and that they are checking all of the results relative to the developer test subset. Note that it might be the case that the test suite is entirely automated, meaning that instead of pre- selecting a subset of the tests, the CCTL instead runs the entire (automated) suite. In this case, the CCTL should select a subset of the results to look at, and then review those according to work unit ATE_IND.2-10. Note that this is equivalent to pre-selecting the subset to run, and so a justification has be given for the selection of the subset of results that need to be examined similar to the one discussed in the paragraph above.

C.5 Vulnerability Assessment (AVA)

C.5.1 Vulnerability Analysis Validation

Work Units EAL2: AVA_VLA.1-2
Work Units EAL3: AVA_VLA.1-2

Validator Guidance: In order to ensure scheme-wide consistency with respect to the somewhat subjective activities listed in work unit AVA_VLA.1-2, the Validator should perform two activities with respect to this work unit. The first is to review the evaluator's analysis of the developer's vulnerability analysis (AVA_VLA.1.1C) and use this review as the basis for analyzing the CCTL's report.

While reviewing the evaluation analysis, the Validator should check that it meets the requirements (that is, obvious vulnerabilities are identified and the rationale detailing why they are not exploitable makes sense).

In the case that a vulnerability is known or identified and the vendor claims that it is not "obvious", the CEM provides a method for determining (for the purposes of AVA_VLA.1-2 only) whether the vulnerability is "obvious" or not. Basically, this method is to use the tables B.3 and B.4 in Annex B of the CEM to make the determination. Because table B.3 has a subjective element to it (that is, the numbers are assigned based on judgment by a human, and not in a strict algorithmic fashion), the Validator should make an assessment as to whether the numbers assigned by the evaluator are correct. If the Validator disagrees with the assessment, the Validator should determine whether the impact of the disagreement would change the outcome per table B.4. Disagreements that do not change the outcome should be noted but not addressed, while disagreements that do have an impact on the outcome should be discussed. However, the Validator is under no obligation to review any changes that are made to either the developer-provided vulnerability analysis or to the evaluator's work with respect to table B.3.

The definition of the term "obvious" is a major issue in terms of this activity. Whether vulnerability is "obvious" or not depends on the expertise of the evaluator, information sources available to the assessor, and of course the opinion of the evaluator. A developer of a piece of software or an expert in a technology area will most likely have a different view of what is "obvious" compared with a new evaluator a first evaluation. Minimally, obvious vulnerabilities are those that are evident from the documentation provided on the TOE as part of this EAL (including design documentation, test documentation, and the vulnerability analysis itself). In addition, there are "publicly available" sources such as Internet sites including rootshell.com, securityfocus.com, etc., and books written on the subject of "hacking." The Validator should use this information to provide guidance to the CCTL in determining what are "legitimate" sources of "obvious" vulnerabilities.

Work Units EAL4: AVA_VLA.2-2

Validator Guidance: The Validator should review the evaluator's analysis of the developer's vulnerability analysis (AVA_VLA.2.1C, AVA_VLA.2.2C) to confirm that

the CCTL has adequately analyzed the developer's analysis, and that the developer has performed a sound analysis as a base for the CCTL. In performing this activity, the Validator should review paragraph 1723 of the CEM, which details three conditions under which a vulnerability could be considered "not exploitable." The Validator should try to choose a sample such that vulnerabilities meeting each condition are sampled, and additionally they need to examine *all* vulnerabilities that are declared non-exploitable as a result of working through Tables B.3 and B.4 in Annex B of the CEM.

Because the values used in these tables are somewhat subjective, the Validator's major purpose is to ensure that 1) these values appear to make sense in and of themselves, and 2) these values are consistent with what other evaluation efforts have used. To this end, the Validator is expected to discuss with the CCTL and developer how the numbers used in the tables were selected, and should consult with other validation reports to learn what numbers were used in other evaluation efforts. The Validator then should document their findings in the validation report so that it may be used by future Validators.

C.5.2 Evaluator Penetration Testing Validation

Work Units EAL4: AVA_VLA.2-11, AVA_VLA.2-12, AVA_VLA.2-15

Validator Guidance: The Validator should review the report produced by the CCTL for work unit AVA_VLA.2-11, and determine that it has the contents listed in the CEM. The Validator should check to see that the tests are sound, and actually test the vulnerability hypothesized. Any changes required of the CCTL by the Validator (including re-writing of documentation and tests) should be reviewed by the Validator to ensure they were implemented. The Validator should summarize the analysis in the validation report. After the test documentation is complete enough to proceed to testing, the Validator needs to observe the penetration testing (called for by work unit AVA_VLA.2-12). This is done with the goal of gaining confidence that the CCTL is performing the tests in the fashion described in the documentation, and that it reacts appropriately to problems or new issues encountered during the testing.

The Validator is responsible for consistency among CCTLs with respect the values used in Tables B.3 and B.4 in Annex B of the CEM. Work unit AVA_VLA.2-15 indicates that the TOE must resist an attacker possessing a low attack potential, which implies that there will be calculations based on these two tables to support this assertion (these calculations will be performed by evaluation CCTL). Therefore, the Validator is expected to discuss with the CCTL how the numbers used in the tables were arrived at, and should consult with validation reports to learn what numbers were used in other evaluation efforts. The Validator then should document the findings in the validation report so that it may be used by future Validators, and provide appropriate feedback to the evaluation CCTL.

C.5.3 Vulnerability Assessment Validation

WorkUnits EAL4: AVA_VLA.2-4, 2-5, 2-6, 2-7, 2-8, 2-9

Validator Guidance: The Validator should note that the EAL4 work units for AVA_VLA.2-4 through AVA_VLA.2-8 describe the CCTL activities in analyzing the vulnerability analysis that the *developer* has performed, while EAL4 work unit for AVA_VLA.2-9 describes an *independent* analysis of the system performed by the CCTL. The Validator needs to review both the output of the CCTL's review of the developer's vulnerability analysis and the independent analysis of the system performed by the CCTL.

(This page intentionally left blank)

C.6 Configuration Management (ACM)

C.6.1 CM Validation

Work Units EAL3: ACM_CAP.3-11
EAL4: ACM_CAP.4-12

Validator Actions: For this item, the Validator is to review the records of the evaluation's CCTL activities in determining that the CM system is being used. In order for the Validator to be able to make an accurate assessment of the CCTL's efforts, the CCTL records must demonstrate a CCTL understanding of the vendors CM documentation and procedures (especially the CM plan: ACM_CAP.3.3.C, ACM_CAP.3.7.C). This activity can be viewed as a "test" of the vendors CM system, and at EAL3 this plays a role in the assurance provided by the TOE. (ACM_CAP.3-11, ACM_CAP.3.8.C)

In performing the Validator action described above, the Validator should determine that the CCTL examines the CM system particularly with respect to the access controls (ACM_CAP.3.10.C) and tracking each CI of the TOE through its life cycle (ACM_SCP.1.2.C). With respect to the access controls, the Validator should determine that the CCTL considers both whether the measures described in the CM seem to be capable of preventing unauthorized access to the CIs, and on whether the vendor seems to be following these procedures. The ACM_SCP-related item requires no action on the part of the Validator other than to be with the contents of the documents, and to discuss with the CCTL its analysis (in the context of performing the Validator action above) to determine that the CCTL's analysis is being performed and checked correctly.

At EAL2 and above the Validator needs to determine that the evaluation confirmed the scope of configuration items the CM system and configuration list must contain. The Validator should review records of evaluation activities for performing the work units related to requirements ACM_CAP.*.4C ("The configuration list shall describe the configuration items that comprise the TOE") and ACM_SCP.*.1C ("The CM documentation shall show that the CM system, as a minimum tracks the following ….."). The evaluation records should explain how the "check that the configuration list uniquely identifies each configuration item" (ACM work units for requirement ACM_CAP.*.6C) was assessed. It is insufficient to just explain the developer's have a unique scheme (which is already covered in the work units for ACM_CAP.*.5C).

For EALs 3 and 4, the Validator needs to determine that the evaluation analysis included looking for duplicate configuration items. If duplicate configuration items are found it could affect the results of other ACM_CAP work units (in particular, the work units for ACM_CAP.*.8C, which requires that the "CM system is operating in accordance with CM Plan").

(This page intentionally left blank)

Annex D. Validation Record Formats

Draft Common Criteria Certificate Information

Memorandum for Record (MR)

Monthly Summary Report (MSR)

Observation Report (OR)

Validation Plan (VP)

Validation Report (VR)

Validator Recommendation

(This page intentionally left blank)

D.1 DRAFT COMMON CRITERIA CERTIFICATE INFORMATION FORMAT

Record Identifier: VIDxxxx-MR-nnnn

DRAFT COMMON CRITERIA CERTIFICATE INFORMATION

Product Name or Protection Profile Name/Identifier:

Version and/or Release Numbers:

Evaluation Platform:

Name of CCTL:

Validation Report Number: (use official report number issued by CCEVS Data/Records)

Date Issued: (this is the date on the Validation Report to be published)

Assurance Level:

Record Author:

Time Spent on this Activity:

(This page intentionally left blank)

D.2 MEMORANDUM FOR RECORD (MR) FORMAT

Record Identifier: VIDxxxx-MR-nnnn

MEMORANDUM FOR RECORD FOR

Product Name (including Vendor) or Title of Protection Profile
CCTL

Record Author:

Type of Activity: Briefly describe the activity or interaction you are documenting. (e.g., bi-weekly status meeting, meeting to discuss test coverage analysis, etc.)

Date of Activity:

Reference(s): List other pertinent records referenced by record identifier.

Participants: If you are documenting a meeting list the attendees, a conference call list the participants, and N/A if you are reviewing documentation, etc.

Activity Inputs: What did you use as input to the activity performed?

Description of Validator Activity: Describe how the Validator performed the activity, what the Validator looked for during the course of a review, rationale, and who was responsible for what, identify the issues that were discussed in meeting, description of evaluation team's position, identification of evidence that was discussed.

Output/Result: (e.g., written comments, verbal guidance provided to team or a decision that is rendered; team concurs with Validator recommendation/decision, team disagrees and wrote an OR)

Observations of team's performance: Does the Validator feel the evaluation team understood the issues being discussed? Is the team relying too heavily on the Validator to assess if the TOE meets the requirements?

Time Spent on this Activity: List the amount of Validator time spent in performing the activity, including the time spent to create this record.

(This page intentionally left blank)

D.3 MONTHLY SUMMARY REPORT (MSR) FORMAT

Record Identifier: VIDxxxx-MSR-nnnn

MONTHLY SUMMARY REPORT FOR

Product Name (including Vendor) or Title of Protection Profile
CCTL
Month and Year

I. Accomplishments

Technical or other project milestones accomplished during the reporting period.

II. Outstanding Action Items

Team, vendor, Validator, or management action items which are not closed. Indicate the responsible party for each item. For tracking purposes, use a consistent numbering scheme from month to month for action items.

III. Technical Issues/Concerns

Include any outstanding technical issues and their expected resolution (if known), a plan for closure, and a date (or evaluation milestone) by which a resolution is needed to avoid a schedule slip.

IV. Management Issues/Concerns

Highlight any areas that should be brought to the attention of management, including where resolution is needed in order to avoid a schedule slip.

V. Project Schedule

Include major project milestones, indicating those that have been completed.

VI. Project Status against Schedule

This is a narrative section about the status of the project against the current evaluation schedule. It should include any schedule slips that have occurred during the reporting period, including a reason, and the likelihood of the project completing on schedule.

VII. Validation Plan

Has the original validation plan been modified during the reporting period? If so, list the new validation plan by record identifier you are now using for the evaluation.

VIII. Records Generated

List the records generated during the reporting period to include filename (record identifier), type of file (word, pdf, etc.), date, author, and contents (witness testing, Validation Plan, kick off meeting minutes, etc.)

IX. Evaluation Evidence

List all proprietary evidence received from the vendor and/or CCTL. Include date received, brief description of item, from whom the evidence was received, who has possession of the evidence, and date and to whom the evidence was returned or how it was destroyed, as appropriate. This log can be referenced as a separate attachment to the MSR.

X. Personnel

List the names, phone numbers, and email address of CCTL evaluation personnel, vendor personnel, and CCEVS assigned personnel who are actively involved in the project.

XI. Improvement Suggestions

As a result of experiences or lessons learned on this project provide suggestions for improving the efficiency or effectiveness of the evaluation/validation process or procedures.

XII. Validation Time

Time (hours) Preparing this MSR: _____
Total Validator Time (hours) this Month: _____
Accumulated Validator Time (hours) this Project To-Date: _____
Projected Validator Time (hours) to Complete Project: _____

D.4 OBSERVATION REPORT (OR) FORMAT

See CCEVS web site at URL: http://niap.nist.gov/cc-scheme/GuidanceDocs.html under "CCEVS Forms & Templates" for an electronic copy of the latest version of CCEVS *Observation Report (OR)* Format.

(This page intentionally left blank)

D.5 VALIDATION PLAN (VP) FORMAT

All planned validation activities will be documented. The Validator will develop this plan after reviewing the application for evaluation acceptance, the security target, the evaluation work plan submitted by the CCTL, and after the CCTL procedures and records orientation. The plan will be reviewed by the Chief Validator for concurrence, and will be presented to the CCTL and Sponsor. The general format for a plan together with a worked example for a TOE evaluation can be found below. The Validator should adjust the Validation plan where appropriate for a PP evaluation.

Worked Example Validation Plan

1. Introduction

This is the Validation Plan for the ABC Product Version 3 EAL4 evaluation being conducted by (Name of CCTL).

2. Evaluation Schedule (to include documentation review and delivery schedule, testing, ETR reviews) **and Validation Activities/Milestones Meetings** (to include purpose, points of discussion and deliverables)

See the *Evaluation Work Plan for ABC Product Version 3, EAL4 Evaluation*, Version 1 dated 1 January 2001
(The evaluation schedule can be here or can be attached or this section can point to the Evaluation Work Plan)

3. Validation Activities/Milestone Meetings

3.1 Product Training Activity

The Validator will attend the 1-day TOE familiarization training held at the CCTL facility in city, state. This activity is further described in Section 4.1on page 14 of the *Evaluation Work Plan for ABC Product Version 3, EAL4 Evaluation*, Version 1.0, 1 January 2001. The purpose of attending the TOE familiarization is for the Validator to obtain a general understanding of the functions and operational characteristics of the TOE to be evaluated.

3.2 Progress & Technical Exchange Meetings

The Validator expects to perform the following activities at the CCTL or vendor site during the course of the evaluation.

A *kick off meeting* will be held at the beginning of the evaluation activity. The purpose of this meeting is to formally accept the product into the Scheme for validation.

An *orientation meeting* will be held immediately following the Evaluation Acceptance Kick-off meeting. The purpose of this meeting will allow the CCTL to provide an orientation to the Validator regarding the quality system evaluation procedures that will be used, and evaluation records that will be kept for the evaluation. Note that the validation team may review the CCTL quality manual solely to determine the CCTL's evaluation procedures and approach for record keeping. The meeting will also enable

the Validator to tour the CCTL facility and to meet the CCTL staff and evaluation team members.

The Validator will attend evaluation progress meetings and technical exchange meetings (TEMs) as needed. This activity is further described in Section 4.7, page 17 of the *Evaluation Work Plan for ABC Product Version 3, EAL4 Evaluation*, Version 1.0, 1 January 2001. The time and days that these meetings will be held are based on the CCTL schedules. The CCTL should inform the Validator of meeting dates and times.

A records review meeting late in the evaluation is expected to be held to allow the Validator to verify the evaluation analysis and conclusions, as needed, for confirming information provided in the ETR.

The Validator will observe the lab as it performs the work units related to *installation of the TOE*. This is to confirm that the team is performing the work units properly with regard to installation and configuration of the TOE.

The *test coverage assessment* meeting will occur near the completion of the evaluation team's test coverage assessment. The validation team will meet with the evaluation team to discuss their test analysis methods and to review the records generated as a result of this activity. The validation team will observe the labs *independent testing activities*.

An optional meeting may occur during the evaluation team's Vulnerability Assessment activities. Depending upon the timing of the vulnerability assessment and product testing, the Validator's review of the vulnerability assessment may occur in conjunction with the product-testing visit, or it may be a separate meeting.

If the CCTL conducts regular *evaluation team meetings*, the Validator will attend those meetings on an as-needed basis. These meetings will facilitate communications with the CCTL and will also allow the Validator to clarify evaluation issues, and to identify areas of interest for other validation activities (records sampling, etc.).

3.3 Review of the Security Target

During the course of the evaluation the ST possibly will be updated and reissued. The Validator will review every major release of the Security Target (ST). The Validator will receive the reissued versions of the ST to keep abreast of what is being evaluated and the security requirements that are being evaluated.

Potential feedback from the Validator on this activity could include:

- The ST evaluation results look good
- Parts of the ST are unclear

(This activity is tied to the ASE aspects of the evaluation)

3.4 Review of Evaluation Work Packages

The Validator will review Evaluation Work Packages (EWPs). The purpose of this activity is so that the Validator can confirm that the Work Packages identified are appropriate and complete for the ST, and review the verdict put forward on particular work units and the supporting rationale of the work unit. The Validator expects the finalized EWPs, as they are finished, to be delivered to the Validator so that they may conduct this review.

Potential feedback from the Validator could include:

- The work package is good (shows rationale and analysis that a certain assurance class is satisfied)
- The work package might not clearly show how a certain assurance class is satisfied (the Validator has questions on how parts of the criteria had been applied during the evaluation).

3.5 Review of Evaluation Procedures and Records

3.5.1 Evaluation Procedures

At the Procedures and Records Orientation meeting the CCTL identified available documented work unit procedures for aaaa, bbbbb, cccccc, ddddd, eeee, fffff, ggggg, hhhhh. An initial review of procedures bbbbb, eeee, fffff, ggggg, and hhhhh was performed and appeared adequate. A more in-depth review of procedures aaaa, cccccc, and ddddd is needed and will be completed before CCTL scheduled use.

The CCTL did not have documented procedures for work units iiiii, and jjjjjj. These procedures will be reviewed before the CCTL scheduled use. The purpose of the review is to gain an understanding of the CCTL methodology that will be used for these work units.

3.5.2 Evaluation Records

Based on the level of information detail that is planned for the ETR it appears that the Validator will need to review the evaluation records that is used to validate the following assurance components:

- ADV_FSP.2
- ADV_HLD.2
- ADV_IMP.1
- ADV_LLD.1
- AGD_ADM.1
- AGD_USR.1

3.6 Functional Testing

The Validator will attend the functional testing that is described in section 4.4, page 15, of the *Evaluation Work Plan for ABC Product Version 3, EAL4 Evaluation*, Version 1.0, 1 January 2001. The Validator will review the Evaluation Work Packages (EWPs) and evaluator test plans that are generated to perform functional testing before attending the functional testing. The purpose of this activity is so that the Validator can observe what type of testing the CCTL is doing to satisfy the functional testing requirements at EAL4

3.7 Penetration Testing

The Validator will review the test plan for penetration testing and witnessing the tests that are conducted in accordance with this plan. This activity is further described in section 4.5, page 16 of the *Evaluation Work Plan for ABC Product Version 3, EAL4 Evaluation*, Version 1.0, 1 January 2001. The Validator would like the EWPs and any tests plans that are generated to perform the penetration testing to review before attending the penetration testing. The purpose of this activity is so that the Validator can observe what type of penetration testing the CCTL is doing to satisfy the penetration testing requirements at EAL4.

3.8 Observation Report Activities

The Validator will work with the CCTL on the drafting and submitting Observation Reports (ORs). The Validator will receive all ORs. The purpose of this Validator activity is to establish a link between the CCTL and the Scheme to express issues with the criteria, methodology or scheme processes used for the evaluation. This activity is used to help move the evaluation to closure.

Potential feedback from the Validator could include:

- The OR is fine for submitting
- The OR is unclear and needs to be recast so that the Scheme may better understand the issue and be able to make a suitable decision.

3.9 Review of CCTL to Sponsor Evaluation Discovery Reports

The Validator will see the evaluation discovery reports to the sponsor, as talked about in Section 4.0, page 13, of the *Evaluation Work Plan for ABC Product Version 3, EAL4 Evaluation*, Version 1.0, 1 January 2001. The purpose of this activity is to ensure that the Validator understands the issues the CCTL is raising with the Sponsor.

3.10 Review of Evaluation Technical Report

The Validator will review the Evaluation Technical Report (ETR). The purpose of this activity is to determine that the ETR accurately reflects the decisions, verdicts, and

outcomes of all the evaluation activities that are conducted during the course of the evaluation.

Potential feedback from the Validator could include:

- The ETR satisfies all of the requirements for an ETR
- The ETR is missing some information or some of the information is not clear and the ETR needs to be updated.

3.11 Review of the Validated Products Listing Entry

The Validator will review the Validated Products List (VPL) entry for the TOE. The purpose of this activity is to see that the VPL is consistent and accurately reflects the evaluation and product description.

4 Validation Records

The CCEVS Validation Identification (VID) for this validation is (insert VID# issued by Records Manager). All records generated by the validation team will be identified using the VID and Record ID. The following types of record IDs are defined for this evaluation.

Memorandum For Record (MR)	VIDxxxx-MR-nnnn
Monthly Summary Reports (MSR)	VIDxxxx-MSR-nnnn
Observation Reports/Decisions (OR/OD)	CCEVS-OR/OD-nnn
Validation Plan (VP)	VIDxxxx-VP-nnnn
Validation Product List Entry (VPL)	VIDxxxx-VPL-nnnn
Validation Report (VR)	VIDxxxx-VR-nnnn

Additionally, updated documents provided by the CCTL to the Validator will be treated as attachments to validation records. This includes versions of the PP (or ST), Evaluation Work Plan, and the ETR. Validation Records submitted by the Validator will typically be provided in Adobe Acrobat format or as MS Word 2000 version 9.0. The OR/OD and final VPL and VR will be delivered in MS Word format.

5 Validation Schedule

6 Contact Information

6.1 Validator

Validator name, email address, phone number

6.2 CCEVS Contacts

Resource Coordinator (Name), email, phone number
Director (Name), email, phone number

Deputy Director (Name), email, phone number

6.3 Sponsor Contact
Sponsor contact (Name), email, phone number
Company name
Address
City, state, zipcode

6.4 CCTL Contacts
Project Manger (Name), email, phone number
Laboratory Manager (Name), email, phone number

6.4 Evaluation Team
Evaluation team leader name, phone number, and other evaluation team member names

(This page intentionally left blank)

D.6 VALIDATION REPORT (VR) FORMAT

NOTE: It has been pointed out that this format is TOE specific. Until a Validation Report format is provided for PP evaluations, the Validator should draw upon this report format, as appropriate, for Validation Reports for PPs.

Validation Report and Its Use

The Evaluation Technical Report (ETR) is written by the CCTL for the Validation Body and serves as the principal basis for the Validation Report. The objective of the ETR is to present all verdicts, their justifications and any findings derived from the work performed during the evaluation, including errors found during the development of the information technology product or protection profile and any exploitable vulnerabilities discovered during the evaluation. The ETR may contain protected information as necessary to justify evaluation results.

The Validation Report is the source of detailed security information about the information technology product or protection profile for any interested parties. Its objective is to provide practical information about the product or protection profile to consumers. The Validation Report need not, nor should contain protected information since, like the Security Target, it contains information for the consumer necessary to securely deploy the evaluated product.

All technical information regarding the evaluation should be drawn from the ETR. The Validation Report shall explicitly state that this information is obtained from the ETR produced by the named CCTL. The technical information stated in the Validation Report shall be stated such that, the Validator, in the interest of NIAP, will remove any biases that may be stated in the ETR.

1 Executive Summary

The executive summary is a brief summary of the entire report. The information contained within this section should provide the audience with a clear and concise overview of the evaluation results. The audience for this section could include developers, consumers and evaluators of secure information technology systems and products. It may be that the reader will be able to gain a basic familiarity with the product or the protection profile and the report results through the executive summary. Some clients, (e.g., accreditors, management) may only read this section of the report, therefore, it is important that all key evaluation findings be included in this section. An executive summary should contain, but is not limited to the following items:

a) Name of the evaluated IT product, enumeration of the components of the product that are part of the evaluation, developer's name, and version;
b) Name of CCEVS CCTL;
c) Completion date of evaluation;

d) Version of the CC;
e) List (or effective date) of the National and International Interpretations applicable to the version of the CC;
f) Version of the CEM;
g) List (or effective date) of the National or International Interpretations applicable to the version of the CEM; and
h) Brief description of the report results:
    1) assurance package;
    2) functionality;
    3) summary of threats and Organizational Security Policies (OSPs) addressed by the evaluated IT product:
    4) special configuration requirements
    5) assumptions about the operating environment
    6) disclaimers; include the statement (use Product or PP as appropriate) "The information contained in this Validation Report is not an endorsement of the [product or protection profile] by any agency of the U.S. Government an no warranty of the [product or protection profile] is either expressed or implied."

2 Identification

The evaluated IT product has to be clearly identified. The software version number, any applicable software patches, hardware version number, and peripheral devices (e.g., tape drives, printers, etc.) must be identified and recorded. This provides the labeling and descriptive information necessary to completely identify the evaluated IT product. Complete identification of the evaluated IT product will ensure that a whole and accurate representation of the IT product can be recreated for use or for future evaluation efforts.

3 Security Policy

The security policy section should contain the description of the IT product's security policy. The security policy describes the IT product as a collection of security services. The security policy description contains the policies or rules that the evaluated IT product must comply with and/or enforce.

4 Assumptions and Clarification of Scope

The security aspects of the environment/configuration in which the IT product is expected to be used in should be included in this section. The section provides a means to articulate the clarification of the scope of the evaluation with respect to threats that are

not countered. Users can make informed decisions about the risks associated with using the IT product. Usage, environmental assumptions, and clarification of the scope of the evaluation with respect to threats that are not countered should be stated in this section.

4.1 Usage Assumptions

In order to provide a baseline for the product during the evaluation effort certain assumptions about the usage of the IT product have to be made. Items such as proper installation and configuration, minimum hardware requirements being satisfied, etc., all have to be assumed. This section documents any usage assumptions made about the IT product during the evaluation.

4.2 Environmental Assumptions

In order to provide a baseline for the IT product during the evaluation effort certain assumptions about the environment the product is to be used in has to be made. This section documents any environmental assumptions made about the IT product during the evaluation.

4.3 Clarification of Scope

This section lists and describes threats to the IT product that are not countered by the evaluated security functions of the product. It may occur that some clients will assume that the product is meeting some threats but in fact they are not. It is for these reasons that these encountered threats should be listed for clarification. It would however, be impractical to list all possible threats that cannot be countered by an individual product.

5 Architectural Information

This section provides a high level description of the IT product and its major components based on the deliverables described in the Common Criteria assurance family entitled Development-High Level Design (ADV_HLD). The intent of the section is to characterize the degree of architectural separation of the major components.

6 Documentation

A complete listing of the IT product documentation provided with the product by the developer to the consumer is listed in this section. It is important that all relevant documentation be noted with the version numbers. The documentation at a minimum describes the user, administration and installation guides. It may occur that the administration and installation guide information is contained in a single document.

7 IT Product Testing

This section describes both the developer and the evaluator testing effort, outlining the testing approach, configuration, depth, and results.

8 Evaluated Configuration

This section documents the configuration of the IT product during the evaluation. Typically, the administrator or installation guide will provide the necessary details for the correct configuration of the IT product. The IT product may be configurable in a number of different ways depending on the environment it is used in or the security policies of the organization that it enforces.

The precise settings and configuration details with accompanying rationale for these choices are outlined in this section. Any additional operational notes and observations can also be included. This section is of particular importance, as it provides a baseline for the evaluated product installation.

9 Results of the Evaluation

This section documents the assurance requirements that the IT product satisfies. A detailed description of these requirements, as well as the details of how the product meets each of them can be found in the Security Target.

10 Evaluator Comments/Recommendations

This section is used to impart additional information about the evaluation results. These comments/recommendations can take the form of shortcomings of the IT product discovered during the evaluation or mention features, which are particularly useful.

11 Annexes

The Annexes are used to outline any additional information that may be useful to the audience of the report but does not logically fit within the prescribed headings of he report (e.g., complete description of security policy).

12 Security Target

The Security Target reference (document identification of the Security Target) and brief summary of ST must be specified.

13 Glossary

The Glossary is used to increase the readability of the report by providing definitions of acronyms or terms of which the meaning may not be readily apparent.

14 Bibliography

The Bibliography section lists all referenced documentation used as source material in the compilation of the report. This information can include but is not limited to:

- criteria, methodology, program scheme documentation;
- technical reference documentation; and
- developer documentation used in the evaluation effort.

It is critical for the sake of reproducibility that all developer documentation is uniquely identified with the proper release date, and proper version numbers.

(This page intentionally left blank)

D.7 VALIDATOR RECOMMENDATION FORMAT

Record ID: VIDxxxx-MR-nnnn

VALIDATOR RECOMMENDATION

Date:

Validation ID:

CCEVS Report Number:

Product:

Based on a review of the CCTL's evaluation results, I recommend that CCEVS accept the (**PASS/FAIL)** verdict from the CCTL.

/s/ Validator name & date

I CONCUR with the Validator's recommendation _____

I DO NOT CONCUR with the Validator's recommendation _____

CHIEF VALIDATOR DATE

I CONCUR with the Validator's recommendation _____

I DO NOT CONCUR with the Validator's recommendation _____

CCEVS DIRECTOR DATE